الإصدار رقم / 17 / - آب - 2011

Augest 2011
Issue 17

Magazine NetworkSet

First Arabic Magazine For Networks



ميسي وكرة القدم والحياة

بعيدا عن النهضة والكلام الفاضي الذي لايغني ولايسمن من جوع وأثناء مشاهدتي لأحد مباريات فريقي المفضل برشلونة ونجمه ميسي وجدت عبرة جميلة ساقتني لكي أكتب عنها مقال اطرح فيه سؤال بسيط «ياترى ماذا سوف يحل بميسي لو توقف عن إبداعه وتوقف عن هز شباك أقوى وأعتد الفرق الأجنبية ؟ وكان جوابي على هذا السؤال سوف يذهب إلى أحد الفرق البسيطة ويلعب بها وقد يدفع له أغنياء العرب المسرفين (حطاب جهنم وبئس المصير) بعض الملايين للعب في فرقهم المجنسة والتى مازالت تصطاد الغربان والتى دائما مايصادف عبورها أثناء تسديد اللاعب على المرمى فيشاهد الغراب في السماء ولايشاهد الهدف الذي أمامه.

لكن أين هي العبرة التى أستوحيتها من كرة القدم وماهو الشيئ الذي أردت أيصاله لكم اليوم, فالحياة وكرة القدم ياقرائي الأعزاء من وجهة نظري شيئان لايختلفان وأنت مطالب دائما بتحديد موقفك ودورك منهم فإما أن تكون مشجع أو لاعب كرة قدم لو في حال كنت شابا يافعا وإما أن تكون مدربا أو حكما في المباراة لو في حال كنت رجل قديرا والعكس صحيح فلقد يكون الرجل القدير ايضا مشجعا في الحياة ويكون من بين الأشخاص الذي لم تعلمهم الحياة شيئ.

المشجع هو الأنسان المستهلك والذي لايملك إلا الكلمات والهتاف والتشجيع والذي لايفكر أبدا في عمل دور إيجابي في حياته غير التشجيع وجملة شكرا , وهذا ما أعتبره إنقاص منك ومن قدراتك , فاللّه أعطانا وأعطاك ميزة فضلتنا عن باقي مخلوقات الأرض ألا وهي العقل وقدراته الغير محدودة وأنتم أيها المشجعون تعتبرون أنفسكم غير قادرين أو محدودي القدرة على فعل شيئ في الحياة يكون له دور إيجابي غير إبتكار الأعذار والمبررات لأنفسكم تحت حجة الوقت والعمل والمسؤوليات والخ... حتى نسيتم أن قدراتكم لاتقل عن قدرات أي شخص آخر وماتحتاجوه هو قليل من العمل والتنظيم , والتدريب لو في حال أردتم أن تكونوا لاعبي كرة قدم.

اللاعب هو الشخص الذي قرر أن يأخذ بزمام المبادرة وقرر فرض نفسه على العالم المحيطة به من خلال العمل الأيجابي والذي يتطلب منه الكثير من العمل والجهد لكي يصل إلى اليوم الذي يضع بصمته فيه ويقول الحمد للّه لقد ساهمت قليلا في التغيير. وإن كان طريقه شاق وصعب جدا إلا أن له نصيب إن لم يكن في الدنيا ففي الآخرة , فالحفاظ على المستوى لمدة طويلة من الزمن وبدون وجود أي دعم حقيقي للأعب سيجعل الكفاءة تقل يوما بعد يوم حتى تتوقف تماما لذلك نجد ميسي يبدع ويتألق بشكل دائم أمام مرمى ريال مدريد والسبب طبعا وجود دعم حقيقي وأقل مايمكننا وصفه بالدعم هو وجود لاعبين محترفين معه يساندونه.

المدرب هم الدعاة والنهضوين الذي يدعون الناس إلى العمل والنهضة وكل يوم نرى داعي جديد وكل يوم برنامج والكل يدعو إلى العمل لكن النتائج وردة الفعل لايستطيعوا التدخل فيها لأن المستمع أو اللاعب هو من سوف يكون في الميدان ولاحظ معي أن الداعي هنا لايستهدف الطبقة المستهلكة فهم لن يتغيروا إلا لو قرروا هذا بأنفسهم لذلك فهو يتحدث إلى الطبقة التى تملك حس التغيير والنهضة من خلال بث المزيد من الطاقات والروح فيهم ويبقى الآداء هو سيد الموقف لأن المدرب في الملعب يقدم الخطة ويحمس اللاعبين ويعدهم بالمكافأة لكن عندما يدخل اللاعب إلى الساحة فهو الوحيد الذي يملك القدرة على التغيير ولاذنب للمدرب لو كان اللأعب لايرى إلا الغربان في السماء عندما يسدد إلى المرمى.

الحكم ياترى من هو ؟ هل يفكرك بشيئ مألوف يتردد صداه في الآونة الآخيرة ؟ نعم هو الحاكم والشيخ والأمير والرئيس والقائد والزعيم , كلهم أوجه لعملة واحدة تتجسد في حكم المباراة فهو صاحب القرار فهو من يعطي الحقوق لأصحابه ويكافئ اللاعبين المجدين ويعاقب اللاعبين المقصرين ويعاقب الجمهور أيضا بحرمانهم من حضور المباراة , لكن لو كان الحكم سيئا سوف يظلمك مرة وأثنان وثلاثة وعشرة لكن هل ياترى سوف يستمر على آداءه هذا وهل سوف يستمر في ظلمه للأعبين المجدين أم أن أحدهم سوف يتغلب عليه ؟ الحكم يغلب في حالة إتحاد اللاعبين جميعهم تحت راية واحدة وهي المصلحة العامة بحيث يؤدي الجميع عملهم بالطريقة الصحيحة حينها فقط سوف نسجل الأهداف ولن يستطيع أي حكم في العالم أن يقول لهم لا!. إلا لو قرر الحكم الوقوف في وجه كل اللأعبين والمشجعين والمدربين حينها سوف تكون النهاية وخيمة وأقل مايمكن أن يحدث له هو طرده من لجنة التحكيم. وخصوصا أن الحكم في دولنا العربية يولد حكما وبعكس دول العالم الآخرى التى يبدأ الحكم حياته كلاعب متميز.

لمقالي هذا عبر كثيرة لا أستطيع إحصائها ولا أستطيع تلخيصها فمازال هناك المباراة نفسها وحارس المرمى كلهم محاور أجد لهم معاني وعبر في الحياة لكن سوف اقول لك شيئ يلخص كلامي كله , ماهو الدور الذي أخترته لنفسك ولماذا ؟ وهل أنت جاهز لنتعاون جميعا على النهضة , فيد واحدة مهما بذلت من جهد لن تثمر كما تثمر جماعة أجتمعت على الهدف الإيجابي فإما أن يخسر الفريق أو يربح ودمتم بود.

أيمن النعيمي - سوريا



Magazine
NetworkSet
First Arabic Magazine for Networks

مجلة NetworkSet مجلة الكترونية شهرية متخصصة تصدر عن موقع www.networkset.net

www.networkset.net

تقرؤون في هذا العدد

احد كنوز سيسكو
Embedded Event Manager



في أول خطواتي في عالم الشبكات عندما كنت اطّلع على المشاكل الفنية التي تحدث في الشبكات، الكثير منها تكون مشاكل بسيطة يمكن حلها ذاتياً من دون تدخل أحد، وهذا ما جعلني أتساءل هل من المعقول أن لا توجد طريقة ما لحل هذه المشاكل بصورة آلية؟ أو على الأقل تسهيل الأمر على مديري الشبكات , وذلك بإعطائهم معلومات عن الأخطاء والتغييرات التي تحصل على الشبكة بشكل آلي .

ومن المؤكد أنه توجد طريقة ما كما كنت أتوقع, فعند حصول خطأ في احد الراوترات أو حصول حدث معيّن مثل تغير في حالة أحد المنافذ أو في أحد المسارات فهناك جهاز سيرفر في الشبكة يكون مسؤول عن متابعة وإدارة هذه الأحداث وإبلاغ مدير الشبكة عن التغييرات التي حصلت وجمع المعلومات وإعطاء التقارير, ويقوم بأخذ الإجراءات اللازمة لمعالجة هذه المشكلة وحلّها, أي يكون عمله كعمل أجهزة السيطرة والتحكم في المصانع .

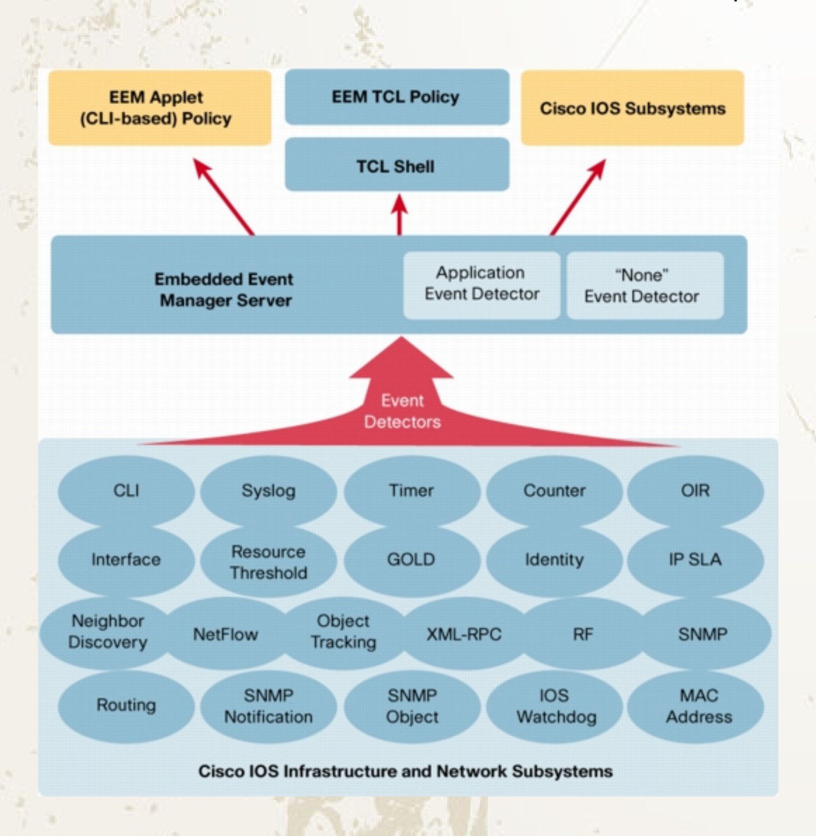
إلى هنا والأمور تسير على ما يرام , ولكن ماذا يحصل لو أن هذه المشكلة كانت في اللنك بين الراوتر والسيرفر, فكيف يكون الحل؟ وكذلك فإن عملية إعادة تشغيل الراوتر عند حدوث مشاكل قد تكلف الكثير بالنسبة لعمل الشبكة وغيرها من المشاكل التابعة .
لذلك لم تتوانى سيسكو وكما عهدناها دائماُ عندما جعلت الراوترات هي نفسها من تقوم بهذه العمليات وقامت بدمج ذلك السيرفر بداخل الراوتر, لذلك جاءت بالمدعو بـ Embedded Event Manager أحد كنوز سيسكو ومحور مقالنا اليوم .

إذن Embedded Event Manager بشكل عام: هو تقنية في نظام تشغيل سيسكو, تسمح لنا بتنفيذ كود برمجي أو مجموعة أوامر عند حصول حدث معيّن. أو بصورة أخرى يمكن اعتبارها كلغة برمجية في نظام التشغيل, تسمح لنا بإضافة وظائف أخرى للنظام وتطويعه حسب رغبتنا.
أتوقع أن الفكرة لم تصل, لذلك سأعرّفه بشكل مباشر, فهي ميزة أو خاصيّة توجد في بعض أنظمة التشغيل الخاصة بسيسكو تجعل الراوتر يتكيف حسب متطلبات المستخدم اعتماداً على الأحداث التي تطرأ على الراوتر, ومن الممكن أن يكون القرار بإرسال إيميل أو بتغيير إعدادات الراوتر مثلاً . آخر إصدار لـ EEM هو 3.1 ضمن نظام تشغيل سيسكو الاصدار 15.0(1)M.

كيف يعمل Embedded Event Manager؟

لنتعرف على طريقة عمله ونلقي نظرة سريعة على مكوناته والتي هي: السيرفر , كاشف الحالات , ومترجم الحالات. المصطلحات قد تكون غير واضحة ولكن لم أجد ترجمة مفهومة اقرب من هذه .
السيرفر: وهو المسؤول عن الربط بين كاشف الحالات ومترجم الحالات.

كاشف الحالات: وهو برنامج يقوم بمراقبة الأحداث والإبلاغ عنها عند مطابقة الحدث مع الشرط وهو يعُتبر عقل الـ EEM، وممكن أن يكون أكثر من نوع مثل : Timer, SNMP, CLI. والإصدارات الجديدة تحتوي على أنواع كثيرة .
مترجم الحالات: يقوم بترجمة الحالة التي انطبق عليها الشرط والمستلمة من كاشف الحالات, وتحديد العمل الذي يجب اتخاذه تبعاً لهذه الحالة, أي ماذا يجب أن ينفّذ عند اكتشاف الحالة. ويكون على نوعين وهما applets و scripts.



ما هي الطريقة التي نبرمج بها الايعازات؟

يدعم EEM ثلاث طرق للبرمجة وهي:

- Applets: وتكون برمجتها مباشرة عن طريق أوامر الـCLI الخاص بالراوتر.
- TCL: هذه الطريقة تستخدم في كتابة البرامج المعقدة وهي تعتبر لغة برمجية بحد ذاتها.
- IOS.sh: ليست كل إصدارات IOS من سيسكو تدعم هذه الطريقة, إنما الإصدارات الحديثة منها فقط، وهي تشبه إلى حد ما كتابة الأوامر في الlينكس عن طريق الـ shell.

مثال لطريقة برمجة applet

كما قلنا إن طرق البرمجة ثلاثة وللاختصار سنقوم بأخذ أول وأشهر طريقة, وهي: applet ونشرحها مع التطبيق، بداية لنفترض أننا نريد أن نجعل الراوتر يرسل لنا إيميل عندما يقوم شخص ما بالدخول عن طريق الـ ssh. ولبرمجة applet للقيام بهذه العملية يجب أن نعمل event يقوم بمراقبة رسائل الـ logالتي يصدرها الراوتر وعند تطابق الحالة المطلوبة يقوم بتنفيذ هذا الـ applet.

أولا يجب أن نعرف رسالة log التي يصدرها الراوتر عند الدخول عن طريق ssh و هي :

```
Dec 17 16:27:53.993: %SEC_LOGIN-
5-LOGIN_SUCCESS: Login Success
[user: cisco] [Source: 172.16.5.2]
[localport: 22] at 17:27:53 Rome Fri
Dec 17 2010
```

الآن يجب تعريف متغيرات الإيميل للراوتر :

```
Cisco(config)#event manager
environment _email_to your-to-mail@
domain.com
Cisco(config)#event manager
environment _email_server your.mail.
server
Cisco(config)#event manager
environment _email_from your-from-
mail@domain.com
```

بعد ذلك جاء وقت كتابة الـ applet:

```
Cisco (config)#event manager applet
login-ssh-ok
Cisco(config-applet)#event syslog
pattern «SEC_LOGIN-5-LOGIN_SUCCESS:
«[Login Success.*[localport: 22
Cisco(config-applet)#action 1.0 mail
server «$_email_server» to «$_email_
to» from «$_email_from» subject «$_
event_pub_time: Login via SSH» body
««$_syslog_msg
Cisco(config-applet)#action 1.5
syslog msg priority 5 «LOGIN SUCCESS
«- Mail Sent
```

دعونا نفصل هذا الـ applet:

الأمر الأول:

```
Cisco(config)#event manager applet
login-ssh-ok
```

event manager applet: لإنشاء الـ applet وتسجيله بداخل EEM.
login-ssh-ok : اسم الـ applet.

الأمر الثاني:

```
Cisco(config-applet)#event syslog
pattern «SEC_LOGIN-5-LOGIN_SUCCESS:
«[Login Success.*[localport: 22
```

event syslog pattern : لتحديد رسالة syslog التي يصدرها الراوتر ليقوم البرنامج بإرسال الإيميل.
وبعدها نكتب الرسالة المطلوبة بين علامتي اقتباس «».
في هذا المثال استخدمنا event من نوع syslog وفي ما يلي أنواع أخرى مثل:
cli : لمراقبة إدخالات الـ cli
ioswdsysmon : لمراقبة الذاكرة والمعالج
nf : لمراقبة أحداث NetFlow
none : يستخدم عندما نريد تشغيل الأحداث يدوياً
snmp : لمراقبة MIB
syslog : لمراقبة رسائل syslog

الأمر الثالث :

```
Cisco (config-applet)#action 1.0 mail
server «$_email_server» to «$_email_
to» from «$_email_from» subject «$_
event_pub_time: Login via SSH» body
««$_syslog_msg
```

action 1.0: وهو العمل الذي يجب اتخاذه عند تطابق الشرط, وهو في هذا المثال يقوم بإرسال إيميل إلى العنوان المحدد بـ $_email_to التابع للسيرفر $_email_server والقادم من $_email_from وعنوان الرسالة يحتوي على وقت الدخول والمتمثل بالمتغير $_event_pub_time إضافة إلى عبارة Login via SSH, أما محتويات الرسالة هي رسالة الـ log نفسها التي حصل عندها الحدث والمتمثلة بالمتغير $_syslog_msg. أما الرقم 1.0 يسمى tag ويستخدم لتمييز العمل المطلوب اتخاذه إذا أدخلنا أكثر من عمل, أما إذا كان إدخال واحد فوضع الـ tag اختياري ويمكن أن يكون أرقام أو حروف ولكن بشروط معينة .

الأمر الرابع :

```
Cisco(config-applet)#action 1.5
syslog msg priority 5 «LOGIN SUCCESS
«- Mail Sent
```

فهو لإنشاء رسالة syslog لإعلام اليوزر بنجاح الدخول وإنه قد تم إرسال إيميل تنبيه بهذه الجلسة .
بعد وصول الإيميل للعنوان المحدد تكون محتوياته كالتالي :
object: Dec 17 19:22:36.203: Login success via SSH
body: Dec 17 19:22:36.195: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user:cisco] [Source: 192.168.10.12] [localport: 22] at 20:22:36 Rome Fri Dec 17 2010

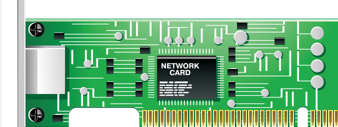
وكذلك في هذا المثال استخدمنا action من نوع mail ومن نوع syslog وفي ما يلي أنواع أخرى مثل:
cli : لتنفيذ ايعازات الـ cli
mail/syslog/snmp-trap/cns-event : لإرسال رسائل mail، syslog، snmp
increment/decrement/append : للتعديل على المتغيرات
if/else/elseif/while/end/break/continue/foreach : العمليات الشرطية
wait : لعمل انتظار
reload/force-switchover : لاعدادات النظام
add/subtract/multiply/divide : معروفة ماتحتاج شرح

ولاستعراض الـ applets المسجلة سابقاً , نستعمل الأمر التالي :
show event manager policy registered
إذا لم يتم كتابة الحدث, فلن يتم تسجيل الـ applet وسوف تظهر رسالة خطأ عند الخروج من applet configuration mode.

في النهاية فإن الـ EEM حقيقةً, يعتبر إضافة رائعة لأنظمة تشغيل سيسكو وسبب اختياري لهذا الموضوع غير السبب السابق, فهو لقلة وجود المصادر الانكليزية التي تشرح الموضوع بشكل وافي لولا موقع سيسكو وايضاً انعدامها في المصادر العربية.
كذلك للعلم فإن لدى سيسكو أكثر من برنامج يقوم بوظيفة مشابهة لعمل EEM مثل:

Embedded Menu Manager (EMM) و Embedded Resource Manager (ERM) و Embedded Syslog Manager (ESM)

ولعلي أحاول في الأعداد القادمة من المجلة إكمال السلسلة. وأعتذر عن الاختصار وعدم التوسع بالأمثلة كون الموضوع متنوع ويحتاج إلى عدة مقالات لتغطيته.





السويتش اللاسلكي أو المتحكم اللاسلكي

Wireless LAN Controller



لمحة عن الكاتب

نادر المنسي

الجنسية : مصر / مقيم بالكويت

مهندس اتصالات يطمح و يساعد في الرقي بالمحتوى العربي للشبكات عبر ترجمة و اعداد مقالات و كتب علمية

naderelmansi@gmail.com

Cisco Catalyst® 6500 Series Wireless Services Module (WiSM)

Cisco 2106 Wireless LAN Controller

Cisco 4400 Wireless LAN Controller





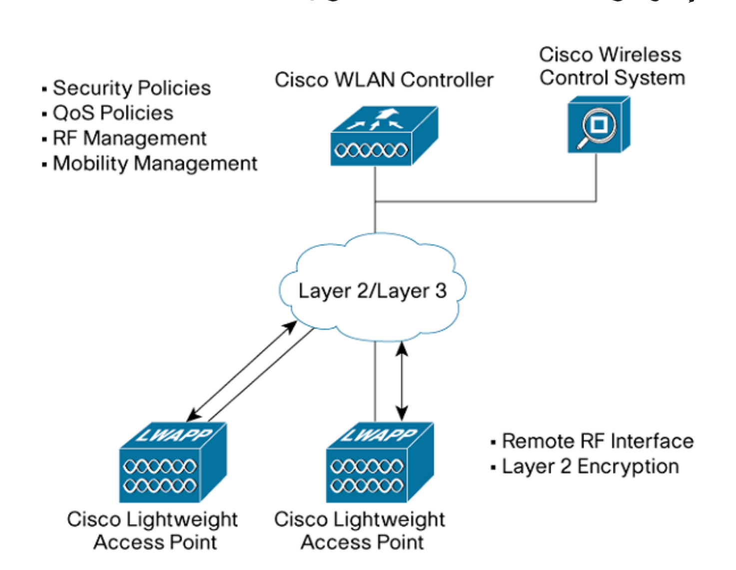
Cisco WLAN Controller Module for Cisco Integrated Services Routers



Cisco Catalyst 3750G Integrated WLAN Controller



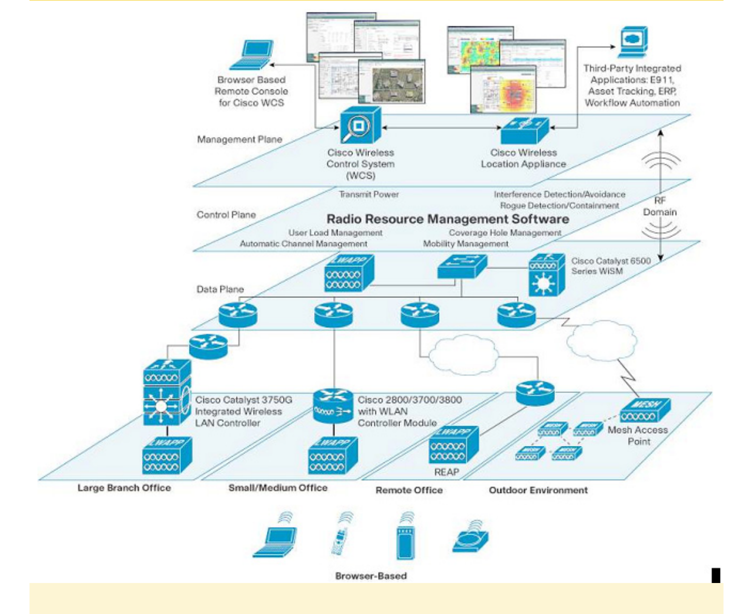
يعمل المتحكم اللاسلكي WLC في البيئة اللاسلكية من سيسكو كعنصر وسيط بين عنصرين آخرين أحدهما أعلى من الآخر , أو بشكل أدق أحدهما يراقب و يدير WLC و هو Cisco Wireless Control System WCS و الآخر تتم ادارته بواسطة WLC و هو نوع خاص من أجهزة الأكسس بوينت تسمى Lightweight AP ويعتبر المكون الرئسي لما يسمى بـ Cisco Unified Wireless Network CUWN و طريقة سيسكو لعمل شبكة لاسلكية , و يقوم بإدارة العديد من أجهزة الأكسس بوينت و تولي مهمة المركزية في الأمن و التحكم و الإدارة و خدمات MOBILITY و Roaming



و عند تعاملنا مع سيسكو فنحن مضطرون للتعامل مع مصطلحاتها, فلن نذكر مصطلح السويتش اللاسلكي هنا كما تطلقه مناهج شركة CWNP بل سنطلق عليه دائماً المتحكم اللاسلكي .

و الكنترولر هو جهاز يقوم بكل وظائف الأكسس بوينت الموجودة في الشبكة و يترك لها فقط مهمة التقاط الإشارة ثم يقوم هو بالمهام التالية :

أولا الإدارة الراديوة للشبكة اللاسلكية



تختلف الشبكات اللاسلكية عن الشبكات السلكية في وجود عوامل أخرى يجب أخذها في الإعتبار عند تخطيط الشبكة و توزيع أجهزتها , و ذلك لإن الإتصال يتم لاسلكياً بواسطة إشارة راديوية قد تعاني من انخفاض القدرة أو التشتت أو الإنكسارات أو غيرها , و لهذا كان على الكنترولر القيام بضبط الإعدادات الراديوية للشبكة و هذه بعضها :

Dynamic channel assignment

هنا يقوم الكنترولر بمهمة توزيع و تنظيم القنوات الترددية و ذلك يعتمد على المعيار المستخدم , فعند استخدام المعيار IEEE 802.11b فيتم توزيع ثلاث قنوات ترددية و هي 1 و 6 و 11 و ذلك لمنع التداخل .

Interference detection and avoidance

في حال لو وجد بعض التداخل فإن اكتشافه و محاولة حل هذا التداخل يعتبر من مهمام الكنترولر

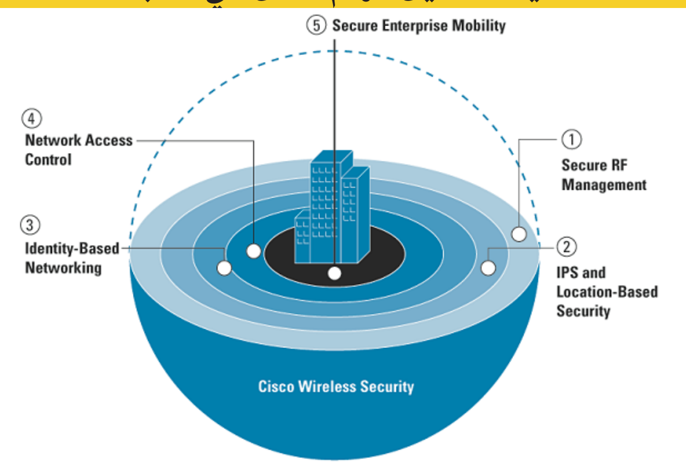
Load balancing

الكنترولر الواحد يقوم بإدارة العشرات من الأكسس بوينت , و قد تتواجد الأكسس بوينت في أماكن لا يتم فيها التوزيع العادل للمستخدمين, مما يزيد الحمل على بعضها دون الآخر , و هنا يتدخل الكنترولر لعمل توزان بين هذه الأجهزة .

Coverage hole detection and correction

حتى و إن قمت بتضييق المسافات بين أجهزة الأكسس بوينت فإنك ستفاجئ بوجود أماكن ميتة لا تستطيع الإشارة الوصول إليها , أو أن الإشارة ضعيفة فيها , وذلك لوجود عوامل مثل : توزيع سيء للأثاث , أو اضطرابات في الطقس , وهنا يقوم الكنترولر بالتغلب على هذه المشكلة بزيادة القدرة للأجهزة المتواجدة في هذه المنطقة وذلك حتى انتهاء هذه المشكلة .

ثانيا : تحسين مهام الأمن في الشبكة



يقوم الكنترولر بتولي مهام الأمن في الشبكات للاسلكية بدلاً عن الأكسس بوينت , حيث يتم تأمين الشبكة عبر تخطيها عدة طبقات كروية لكل منها طريقة تأمين خاصة بها , كما يبينها الشكل السابق .

الدائرة الأمنية الأولى RF security

في هذه الدائرة يمنع الكنترولر الأجهزة اللاسلكية من استقبال أي اشارة خارج نطاق الشبكة و يكون هنا الأمن معتمداً على الطبقة الأولى في طبقات OSI وهي physical ويتم ذلك عبر اختيار معايير لاسلكية من a , b , g , n .

الدائرة الأمنية الثانية Wireless LAN intrusion prevention, location, and correlation

لا يقتصر دور الكنترولر على منع الأجهزة والإشارات الغريبة عن الشبكة من الولوج إليها , بل يقوم بمنع الإشارات و الأجهزة المصابة ببرمجيات خبيثة والتي لها صفات فيروسية من الدخول للشبكة , و ذلك لكون الكنترولر يحتوي على خدمة داخلية شهيرة في الأمن الشبكي وهي intrusion-detection-system IDS والتي توجد كأجهزة أو برمجيات متخصصة , وهي هنا كخدمة داخلية في أجهزة الشبكات اللاسلكية يقوم عليها عبء تحليل الإختراقات وعزل الأجهزة التي تتورط في هذه المشكلات

الدائرة الأمنية الثالثة Identity-based networking

هنا يتم تأمين الشبكات اللاسلكية بالإعتماد على التكامل بين الكنترولر والأجهزة الشبكية الأخرى مثل السويتشات والراوترات والتي تستخدم في الربط بين الأكسس بوينت و الكنترولر أو الربط بين أجهزة الكنترولر ببعضها البعض . ويتم تأمين الشبكة اللاسلكية عبر بروتوكولات الطبقة الثانية data link layer 2 مثل 802.1x و 802.11ا مثل wpa , wpa2 .

أما الطبقة الثالثة Network layer 3 فيتم التعاون فيها مع سويتشات وراوترات الشبكة لعمل إعدادات VLAN و التي تعتبر من أهم اعدادات الشبكة اللاسلكية لضمان انعزالية ترافيك البيانات وترافيك ادارة الشبكة .

في الطبقة الثالثة أيضا يتم التأمين بواسطة ACL و ذلك لمنع أو السماح لنطاق ايبيهات معينة من المرور في الشبكة او استخدامها ,

و تعتبر أيضا إعدادات QOS من خصائص الطبقة الثالثة و التي يتم فيها عمل تفاضل بين أنواع البيانات المارّة و هي و إن كانت في الأصل ليست من طرق الـتأمين إلّا أن الشبكة اللاسلكية تعتبرها كذلك .

و الأهم في هذا كله أن الطبقة الثالثة في OSI يقع على عاتقها التأمين الأحترافي و المسمى RADIUS و الذي يلقي بعملية التأمين على سيرفر خاص network access server (NAS) يتكامل مع الكنترولر ليقوم بإعطاء التراخيص للمستخدمين عبر عدة عمليات تسمى Authentication, authorization, and accounting (AAA) .

الدائرة الأمنية الرابعة Network Admission Control NAC

و هي النسخة (السيسكاوية) من تقنية أمن الشبكات Network Access Control و التي يتم فيها الترتيبات النهائية لوصول المستخدم إلى الجهاز الشبكي , حيث يعمل كـ network access server (NAS) بالإضافة إلى مهمة firewall. في المرحلة النهائية للدخول يعتمد على هوية العميل المدرجة في قواعد بياناته للسماح له بالدخول.

أنواع الكنترولر

لدينا ثلاث أنواع من أجهزة الكنترولر هم :

Standalone controllers

وهنا يكون الكنترولر جهاز طبيعي قائم بذاته مثل الراوتر أو السويتش و بحجم 1 rack unit و من أنواعه Cisco 4400 Series و Cisco 2106 Wireless LAN Controllers

integrated controllers

يتم هنا دمج خصائص الكنترولر في بعض أجهزة الشبكة لتعمل ككنترولر و ذلك كمهمة إضافية , و يعتبر سويتش CiscoCatalyst 3750G أهم مثال على ذلك, لإحتواءه على كنترولر يسمى Cisco Catalyst 3750G Integrated Wireless LAN Controller و لكن لابد أن تعلم أن سويتشات 3750 بعضها يأتي مدمج و البعض الآخر يأتي خالي من هذه الخاصية و ليس هناك مجال لترقيته , و لهذا عند شرائك الجهاز يجب أن تحدد المواصفات التي تحتاجها .

modular WLAN controllers

و هنا يتم وضع موديولات داخل أجهزة الشبكة كي تضيف إليها مهمة الكنترولر كمهمة إضافية لها مثل سويتش Cisco Catalyst 6500Series الذي يتقبل موديولات Cisco Catalyst 6500 Series WiSM و (Cisco Wireless LAN Controller Module(WLCM لتعمل ككنترولر .

تختلف هذه الأنواع في بعض الخصائص فتتميز modular WLAN و integrated controllers controllers في كونها تدعم خصائص مميزة في السويتشات و الراوترات مثل ACL و VLAN و غيرها من الخدمات التي قد تحتاجها الشبكات اللاسلكية و كذلك فإن الكنترولر سيستفيد من كامل الخصائص الفيزيائية و خصائص الراوتينج و السويتشنج للسويتش

و تختلف أيضاً في مدى دعمها لعدد أكثر من الأكسس بوينت و كيفية إدارتها و عدد المخارج التي تدعمها للربط مع أجهزة الشبكة الأخرى .



و هذه مقارنة شاملة بين جميع أنواع الكنترولر التي تصنعها سيسكو

المنتج	الخصائص	الشبكات التي يدعمها
	Wireless LAN Controllers	
Cisco 2106 Wireless LAN Controller	يستطيع إدارة ستة أكسس بوينت مخرجان لدعم poe مخرجان uplink	يدعم الشبكات الصغيرة
Cisco 4400 Series Wireless LAN Controller	دعم 12 و 25 و 50 و 100 اكسس بوينت الموديل 4402 يحتوي على مخرجان جيجا ايثرنت أما الموديل 4404 يحتوي على أربع مخارج جيجا ايثرنت يحتوي على خصائص spanning tree و IPSEC محصن ضد تداخلات الموجات الكهرومغناطيسية	موجه للشبكات المتوسطة و الكبيرة
	Wireless Integrated Switches and Routers	
Cisco Catalyst 6500 Series Wireless Services Module (WiSM)	دعم300 اكسس بوينت يحتوي على خصائص IPSEC محصن ضد تداخلات الموجات الكهرومغناطيسية.	يدعم الشبكات الكبيرة حيث أن سويتش 6500 يتواجد في هذه الشبكات
Cisco Catalyst 3750G Integrated Wireless LAN Controller	دعم 25 و 50 اكسس بوينت حسب الموديل الداخلي يحتوي على خصائص IPSEC محصن ضد تداخلات الموجات الكهرومغناطيسية.	للشبكات المتوسطة الحجم
Cisco Wireless LAN Controller Module for Cisco Integrated Services Routers	و يتم قبسه في أجهزة راوترات 3800,3700 , 2800 يستطيع إدارة ستة أكسس بوينت	الشبكات الصغيرة و المتوسطة



Magazine NetworkSet

First Arabic Magazine for Networks

معنى جديد لعالم الشبكات في سماء اللغة العربية









انقر على صورة المشروع
لزيارة صفحته على شبكة الانترنت



الفرق بين بروتوكول IPSEC و SSL

لمحة عن الكاتب
أنس المبروكي
الجنسية : المغرب
23 سنة. مهندس في الشبكات والأنظمة (EMSI- Rabat)
CCNA R&S ,CCNP R&S
mabroukianas@gmail.com

هل سألت نفسك كيف يمكننا الحجز في الفنادق وشراء العديد من الأشياء عن طريق الإنترنت بواسطة الفيزا كارد أو الماستر كارد و بأمان تام ؟، وكيف يتم دخول بعض موظفي الشركات من منازلهم إلى الشركات والحصول على حماية بياناتهم من القرصنة ؟ . كل هذا يتم عن طريق تقنية Remote Access VPN .

التعريف الكلاسيكي لـ Virtual Private Network (VPN)) : هو حدوث اتصال آمن بين مقرين للشركة , مثلاً بين المقر الرئيسي ومقر فرعي , ويمر هذا الاتصال عبر شبكة عامة كالإنترنت مثلاً .ويمكن تصنيف برتوكولات الـ VPN إلى مجموعتين : برتوكولات Site-to-Site VPN و برتوكولات Remote Access VPN .

تسمح بروتوكولاتSite-to-Site VPN لشركة ما بربط الاتصال بين فرع الشركة الأم وفروع الشركة المتواجدة في أماكن بعيدة حتى يتمكن فرع الشركة الأم من تبادل وإرسال البيانات مع الفروع الأخرى بطريقة آمنة وذلك عن طريق تشفير البيانات المتبادلة بينهما. وعن طريق بروتوكولات Site-to-Site VPN يمكن ربط الشركة مع فروعها وهو ما يسمى بالـ Intranet VPN ، كما يمكن ربط الشركة مع شركائها , وهو ما يصطلح عليهExtranet VPN , وهذا كله لإلغاء استخدام الخطوط المؤجّرة (leased lines)الممنوحة من قِبَل موزعي الإنترنت وذلك لتكلفتها الباهظة . ومن بين أبرز بروتوكولات Site-to-Site VPN نجد :

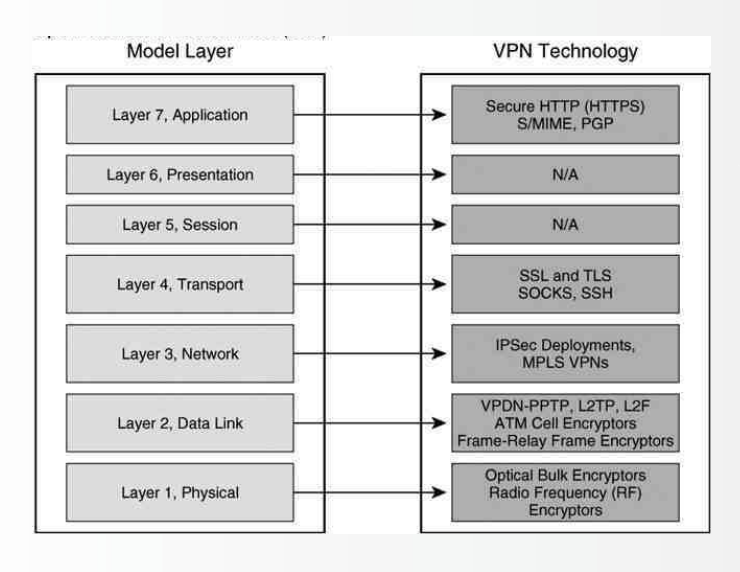
Internet Protocol Security(IPSec), Generic Routing Encapsulating(GRE), Multi-Protocol Label Switching(MPLS) VPN .

أمّا فيما يخص برتوكولات Remote Access VPN التي سأركز عليها في هذا الموضوع فهي تمكن موظفي الشركات من العمل من منازلهم أو أي مكان في العالم) بالنسبة لبعض البرتوكولات (و الدخول إلى شبكة الشركة واستعمال الـservers ressources و الـ applications كأنهم مرتبطين مباشرة بالشركة , كما يمكنهم استخدام الهاتف وإجراء المكالمات وكأنهم بداخلها.

في و.م.أ و أوروبا تستعمل العديد من الشركات هذه التقنية لتمكين الموظفين من العمل داخل بيوتهم , وتسمى هذه الشركات : الشركات الإفتراضية Virtual Entreprises. وهناك العديد من البرتوكولات التي تمكّننا من عمل Remote Access VPN ونذكر منها : IPSec, SSL, L2TP(Layer 2 Tunneling Protocol), PPTP (Point-to-point tunneling protocol), L2TP over IPSec سنركز في هذا الموضوع على IPSEC و SSLولكن سنقوم بتعريف بسيط للبروتوكولات الأخرى .

- PPTP : صمم من طرف شركةMicrosoft ويستخدم برتوكول TCPمنفذ رقم /1723 /
- L2TP : يجمع بينL2F من شركةCISCO و PPTP شركةMicrosoft ويستخدم برتوكول UDP منفذ رقم . /1701/
- L2TP over IPsec : لا يوفر حماية قوية للبيانات . للحصول على هذا الهدف نستخدم معه IPSEC.

وهذا رسم بسيط يوضح مكان تقنياتVPN على . OSI MODEL



- IPSecهو عبارة عن مجموعة(framework) من بروتوكولات Security ، يعمل في المستوى الثالث لـ Model OSI وهو من بين تكنولوجياVPN المستخدمة على نطاق واسع . تم تصميم الـIPSEC لضمان سلامة البيانات(Data Integrity) لكي لا يتم تعديلها أثناء الإرسال، وللحصول على الـAuthentication وذلك بالتأكد من أن البيانات تأتي من مصدر موثوق به ، وتشفير البيانات (Data encryption) لضمان سرية المحتوى .

يتكون الـIPSEC من خمس لبنات أو مستويات :

الأول يمثل بروتوكول IPSEC . وتشمل خيارات الـ AH Authentication Header أو الـESP Encapsulation Security Payload . يوفر الـ ESP الـ Authentication ، سلامة البيانات Data Integrity وتشفير البيانات Encryption , بينما يوفر الـ AH الـ Authentication سلامة البيانات Data Integrity فقط.

الثاني يمثل نوع الـConfidentiality المستخدمة باستعمال خوارزمية التشفيرEncryption Algorithm مثلDES، AES ،3DES ، أوSEAL . الاختيار يعتمد على مستوى الحماية المطلوبة .

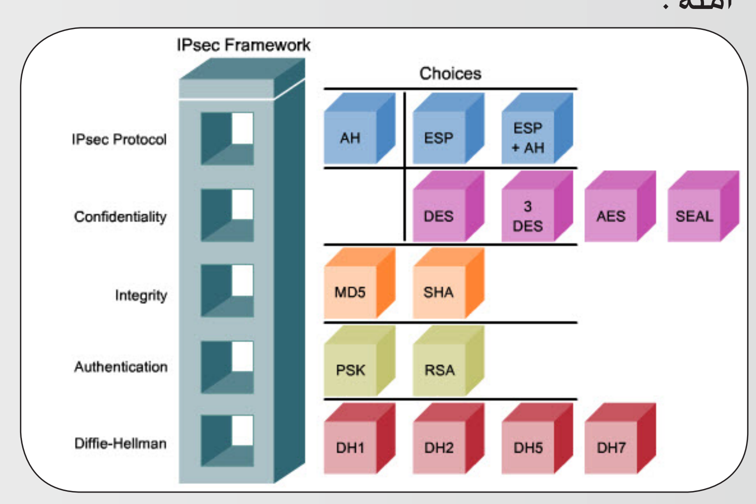
الثالث يمثل سلامة البيانات DATA Integrity, والتي يمكن تنفيذها إمّا باستخدام MD5 Message Digest 5 أو SHA Secure Hash Algorithm .

الرابع يمثل كيفية إنشاء المفتاح السري المشترك.

هناك طريقتين : الـRSA Rivest Shamir Adleman أو الـPres Shared Key

الأخير يمثل مجموعة DH . هناك أربعة مجموعات لتبادل مفتاح التشفير , من بينها : DH3 ، DH2, DH 1 ، و DH7

DH : هي طريقة لتبادل المفاتيح العامة , وهي وسيلة توفر لاثنين من الـDevices لإنشاء المفتاح السري المشترك ، على الرغم من أنهم في اتصال على قناة غير آمنة .



الـIPSec : يوفر مجموعة من البروتوكولات , وللـAdmin الحق في اختيار البروتوكولات المناسبة .

يمكننا استخدام الـ ESP و الـ AH في طريقتين مختلفتين : Transport mode و Tunnel mode

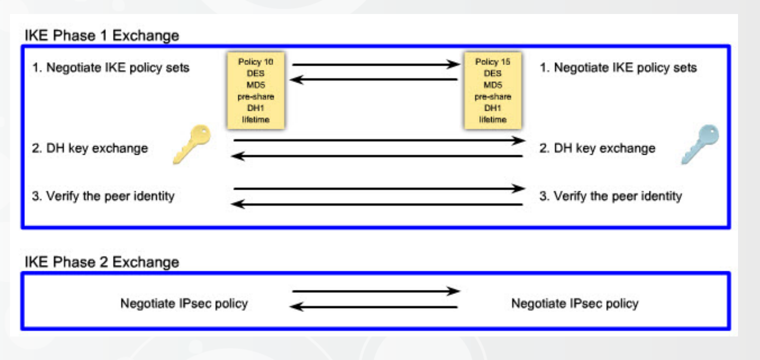
Transport Mode : يتم توفير الأمن و الحماية في Transport layer وما فوق . لكنه يترك الـNetwork layer بدون تشفير . ويستخدم عنوان الـ IP الأصلي لتوجيه الحزمة من خلال الإنترنت. وهو يستخدم بين الحواسيب.

Tunnel mode : يوفر الحماية للـIP packet بشكل كامل . يتم تشفير الـIP Packet الأصلية ويضعها في IP Packet جديدة. يستعمل الـ Tunnel mode بين الكمبيوتر و الـVPN Gateway , أو بين VPN Gateway و VPN Gateway آخر .

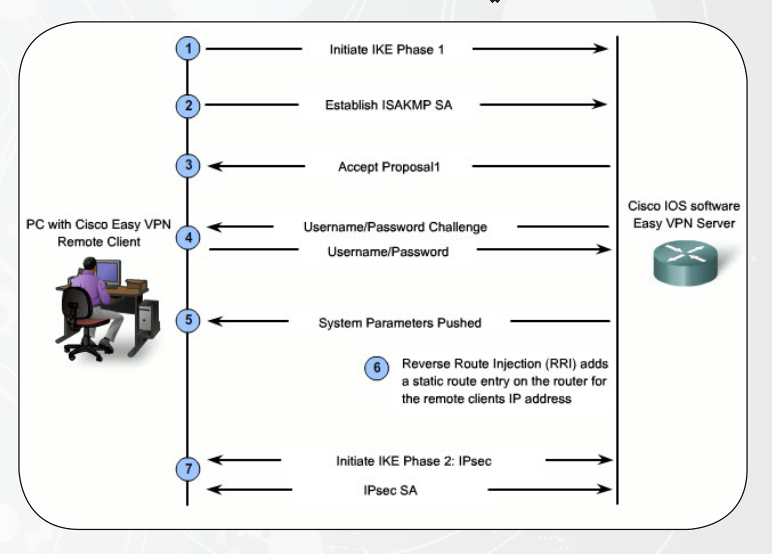
IPSEC يعمل على تفاوض على تبادل المفاتيح ويضع مفتاح مشترك،(authenticate the peers (the devices ،ويتفاوض على خوارزميات التشفير. كل هذا يسمى بـ Security association .

الـ IPSEC يستخدم بروتوكول الـ Internet Key Exchange(IKE) للحصول على قناة آمنة للتواصل , و يقوم البروتوكول بهذا الشيء على مرحلتين :

- المرحلة 1: الـDevices يتفاوضون على Security association. الغرض الأساسي من المرحلة 1 هوالتفاوض على الـIKE policy sets ، عمل authentication لـ peers وإنشاء قناة آمنة بين الـDevices .
- المرحلة 2: التفاوض حول الـ Security association.



وللحصول علىIPSec session آمنة تحدث عدة مراحل استباقية بين الـ Client VPN و الـVPN Gateway . ويوضح الرسم التالي هذه المراحل :





1. الـvpn client يبدأ المرحلة 1IKE phase
2. تؤسَس SA ISAKM , تشمل على مجموعة من خوارزميات التشفير و خوارزميات الـ HASH ، طريقة الـ Authentication و رقم مجموعةDH .
3. الـ Vpn plateforme (router) تقبل اقتراح SA .
4. الـ Vpn plateforme (router) تعرض على الـ client لإتمام عملية الـauthentication وذلك بإرسال الاسم وكلمة السر.
5. الـ Vpn plateforme (router) تقوم بتزويد الـ client بالـ IP adress وdns و إعدادات أخرى .
6. تبدأ عملية الـ RRI (reverse route injection) بإضافة static route للـIP adress الداخلية للـvpn cleint .
7. تم الوصول إلى قناة آمنة لتبادل البيانات بعد أن تم إتمام الـ SA.

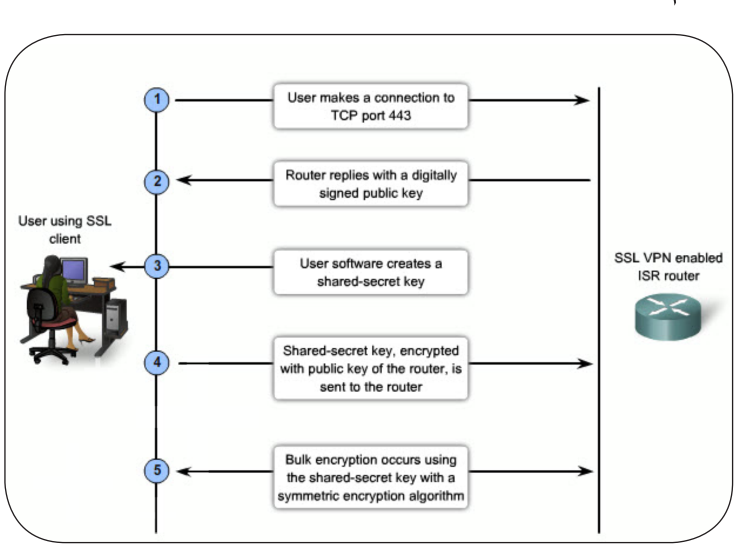
- SSL(Secure Socket Layer) :

تم تطوير هذا البروتوكول من قبل Netscape لتوفير الحماية للمواقع التجارية الالكترونية التي تتطلب تشفير البيانات . على الرغم من أنه قد صمم َ لتوفير وصول آمن على شبكة الإنترنت (web Access) , وقد تم الاستفادة من هذا البروتوكول على نحو متزايد , وذلك بتوفير وصول آمن إلى التطبيقات المستخدمة بشكل شاسع، كالـ.. Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), Internet Message Access Protocol (IMAP). و الـFile Transfer protocol (FTP)

VPN SSL : متوفر بسهولة في كل متصفحات الويب تقريباً , كما يمكنك التنقل بأمان فيv صفحات الويب الداخلية للشركة ، أو حتى فتح البريد الإلكتروني الخاص بك في الشركة .

وللحصول على SSL session آمنة , تحدث عدة مراحل استباقية بين الـ Client VPN و الـVPN Gateway .
ويوضح الرسم التالي هذه المراحل :

1. يفتح المستخدم اتصال على TCP إلى منفذ 443 الذي هو خاص بالـ HTTPS و الذي هو بروتوكول يجمع بين الـ HTTP و الـ SSL .
2. يرد الـ VPN Gateway و الذي يعبر هنا عن روتر بمفتاحه العام .
3. يقوم الـ cleint بإنشاء مفتاح سري مشترك و الذي سيستخدم فيما بعد بين كلا الطرفين لتشفير البيانات .
4. يتم تشفير المفتاح السري المشترك باستخدام المفتاح العام للـVPN Gateway وإرساله إليه .



5. الآن الـ Client و الـ VPN Gateway متفقان على المفتاح السري المشترك , إذن تشفير البيانات يمكن أن يحدث دون مخاوف.

في الجدول التالي سأوضح بعض الفروقات الأساسية بين الـIPSEC و الـ SSL .

الخاصية	IPSEC	SSL
Application	كل الـIP based Applications	Web enabled Applications File sharing , email., يمكن تحقيق ALL ip based Applications لكن هناك بعض التعقيدات في الـ interoperability
برنامج الـ Client	Client Based Technology يجب علينا تثبيت برنامج خاص كالـCisco easy VPN client على أجهزة الموظفين وهذا ما يزيد علينا ثمن رخصة البرنامج ويضيف على الـ Admin عمل إعدادات الـ Clients	Clientless Technology يمكننا من أي Browserأن ندخل إلى Resources
Business	يعمل جيدا للـRemote Access الخاص بالموظفين	يبسط عملية الـ business partner access
Access	نتحكم ونعرف مسبقاً الـ Clients	يمكننا من الدخول من أي مكان من أجهزة غير مسيرة وهذا يمثل نقطة ضعف في Security لإننا لا نتحكم و لا نعرف الـ Clients
البرتوكولات المستخدمة في التشفير	DES, 3DES, AES,SEAL	DES, 3DES, RC4128-, RC440-, AES
طول الـ Keys	56 bits -> 256 bits	40 bits -> 128 bits
الإستخدام	على نطاق واسع	نمو بسرعة عالية

للتذكير فقط : كِلا البرتوكولين IPSECو SSL يستخدمان Symetric Encryption , يعني نفس المفتاح للتشفير ولفك التشفير , وذلك لسرعة تقنية Symetric Encryption بالمقارنة مع Asymetric Encryption , وعدم استهلاكها لنسبة عالية من memory و CPU . وبهذا نكون قد انتهينا وشكراً وأتمنى أن ألقاكم في موضوع آخر إن شاء اللّه , حفظكم اللّه .

كتاب أعجبني

منذ ان بدأت فى كتابه بعض المقالات عن التشفير تلقيت بعض الرسائل من اشخاص مهتمين بهذا الفرع , اغلبهم كان يسأل عن مصادر تعليميه لهذا الفرع , لهذا خصصت هذا الجزء الذى اتمنى ان يكون باب ثابت فى المجله بعنوان «كتاب أعجبنى» للحديث عن كتابين مهمين فى هذا المجال , و اتمنى ان يشجع هذا الموضوع على القراءه .

الكتاب الاول : اسم الكتــــاب : Cryptography For Dummies

اللغة : الانجليزية   اسم المــؤلف : Chey Cobb

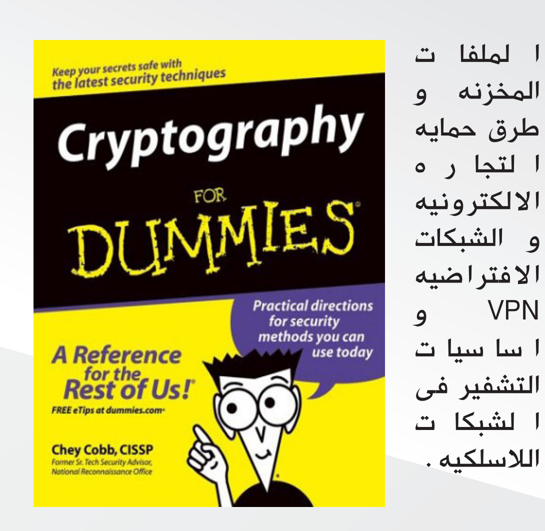
سنه الاصــــدار : 2004   عدد الصفحات : 336

نبذه عن الكتاب :

كتاب Cryptography For Dummies ينتمى الى عائله شهيره من هذا النوع من الكتب , سبب اختيارى له هو امتيازه بطابع من البساطه فى شرح المواضيع و الاستعانه بالكثير و الكثير من الامثله مما يجعل القارىء لا يمل بفيض من المعلومات المقدمة له , فبرغم من قدم هذا الكتاب الا انه يعتبر مصدر ممتاز للبدايه فى مجال امن المعلومات خاصه فرع التشفير , هذا الكتاب موجه بشكل اساسى الى القارىء المبتدىء المهتم بالبدايه فى مجال التعميه و التشفير , لذلك فستجد الكثير من المفاهيم المصحوبة بامثله للتوضيح باعتبار ان القارىء ليس لديه اى خلفيه عن الموضوع .

شىء اخر نجحت مؤلفه هذا الكتاب فى تحقيقه و هو عندما يتحول كتاب علمى تقرأه الى مجرد كتاب مسلى و ممتع تتمنى ان تصل الى اخره , و كما قلت سابقا سبب ذلك هو تقديم المعلومة بطريقه غير مباشره و الاستعانه بالكثير من الامثله و التى يكون بعضها طريف فعلا .

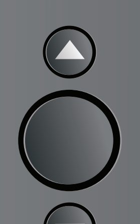
الكتاب مقسم الى اربعه اجزاء , كل جزء يضم مجموعه من الابواب , الجزء الاول منه و هو الاروع حيث يبدأ معك فى علم التعميه و يشرح المصطلحات المهمه فى كل من امن المعلومات بشكل عام و التعميه و التشفير بشكل خاص , بعد قراءه هذا الجزء يكون لديك خلفيه جيده عن الموضوع . اما الجزء الثانى فهو خاص ب Public Key Infrastructure و تم الشرح هذا الموضوع بشىء من التفصيل خلال هذا الجزء . الجزء الثالث يتناول تقنيات التشفير المستخدمة فى الواقع العملى مثل عمليه تشفير البريد و حمايه الملفات المخزنه و طرق حمايه التجاره الالكترونيه و الشبكات الافتراضيه VPN و اساسيات التشفير فى الشبكات اللاسلكيه .

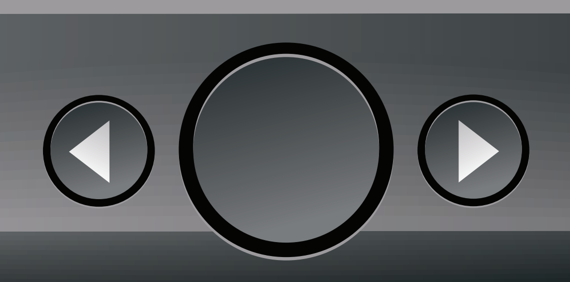


الجزء الرابع و الاخير فهو يحتوى على بعض النصائح و التعليمات و يحتوى على اهم المصادر التعليميه فى هذا المجال و اشهر المواقع و البرامج التى قد تستفيد منها .

ملحوظه اخيره قدم الكتاب لا يدل على انه غير مفيد , مطلقا , علوم التعميه و التشفير تختلف بعض الشىء عن باقى المجالات التقنيه سريعه التطور لان الخوارزميات و التكنيكات الخاصه بهذا الفرع لا تتطور بشكل سريع حيث تمر بالعديد من الاختبارات من مجتمع ال Cryptography حتى تثبت الخوارزميه قوتها ومثال على ذلك خوارزميه DH التى تستخدم حاليا تم نشرها عام 1976 و مازالت من اقوى الخوارزميات الى الان .

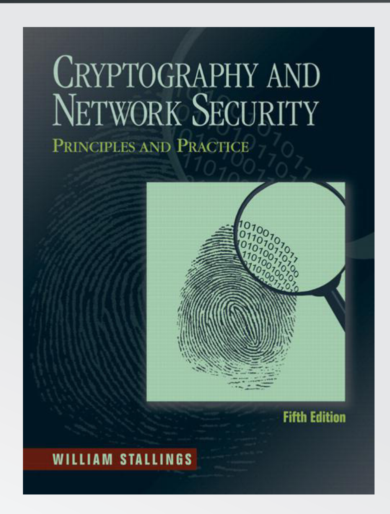
الخلاصه : كتاب متميز سهل الفهم و الاستيعاب موجهه للقارىء المبتدىء و لا يدخل فى التفاصيل الدقيقه و العمليات الرياضيه المعقده التى تهم المتخصصين و مناسب كخطوة اولى .







الكتاب الثاني :



اسم الكتـــاب :
Cryptography and
Network Security
اللغـــــــه : الانجليزية
اسم المـؤلف : William Stallings
رقم الاصــدار : الاصدار الخامس
سنه الاصدار : 2010 عدد الصفحات : 744

نبذه عن الكتاب :

اذا كنت تبحث عن ماده علميه مفصله اشبه بمرجع علمى فهذا الكتاب مناسب لك , فهذا الكتاب يحتوى على كم كبير من المعلومات الخاصه بعلم التعميه و بعض المفاهيم الخاصه بامن الشبكات , و لأن معظم الكتب المتعمقة فى التشفير يكون معظمها موجه الى المبرمجين فهذا الكتاب موجه الى مهندس الشبكات المهتم بالمجال , الكتاب يحتوى على العديد من المصطلحات الرياضيه و التفاصيل التى تهم من يحاول التعمق .

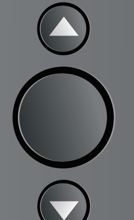
الكتاب مقسم يحتوى على عشرين باب مقسمين بدورهم على اربعة اجزاء , الجزء الاول بعنوان Symmetric Cipher و يخوض فى التشفير التناظرى و خوارزمياته , و يضم سبعه ابواب , الجزء الثانى من الكتاب بعنوان Public-Key Encryption and Hash Functions و به الكثير من المعلومات عن التشفير الغير تناظرى Asymmetric و ايضا عن التوقيع الالكترونى و تقنية ال Hashing . و الجزء الثالث بعنوان Network Security Applications و يتكلم عن بروتوكولات الشبكات و طريقه الحمايه التى تتبعها و هو اقرب الى مجال الشبكات من التشفير , و الجزء الرابع و الاخير بعنوان System Security و هو اشبه بالباب السابق فهو عن امن و حمايه الشبكات ايضا ولكنه يتحدث عن انظمة الامن والحمايه مثل الجدران الناريه و الديدان و الفيروسات و الهجمات الموجه الى الشبكه .

هذا الكتاب يعتبر خطوة ثانيه بعد الانتهاء من الكتاب الاول , شىء مهم جدا فقبل ان تحاول ان تقرأ هذا الكتاب يمكنك قراءه اجزاء معينه تريد فهمها ليس اكثر , اما اذا كنت تريد قراءه الكتاب كله من الغلاف الى الغلاف فستضطر بذل الكثير من الجهد لان هناك اجزاء معقده بحق , لذلك ان لم تستوعب جزء معين يمكنك تركة و الانتقال الى جزء اخر .

الخلاصه : كتاب مفصل و متعمق بعض الشىء فى التشفير و به العديد من المواضيع الخاصه بامن الشبكات و موجه بنسبه اكبر الى المتخصصين عن المبتدئين .















FTP Anatomy

إحدى مشاكل الـ security هو تعامله مع العديد من البروتوكولات التي تعتمد كل منها طريقة في العمل , من أهم النصائح التي يجب الإلتزام بها في مجال الـ security و إتباعها للوصول إلى الحد الأقصى من الحماية هي كالآتي «السماح بما نحتاج فقط و عدم تفعيل أي شيء أو السماح بمرور ما لسنا في حاجه إليه وضماناً لحد الأدنى للصلاحيات»ولتوضيح هذا الكلام النظري سأستعين بمثال عملي , يوجد لدينا شبكة بها عدة سيرفرات منها http»» ومنها«ftp » وهنا كمجموعة مستخدمين يحتاجوا إلى الولوج إلى هذه السيرفرات عن طريق الانترنت مثلا , في حالة كهذه سنحتاج إلى تطبيق ACL على الـ Interface المواجه للانترنت للسماح لها بالإتصال إلى هذه السيرفرات فقط عن طريق Ports»» معيّن هو ومنع أي «»traffic غير ذلك , بهذا قد نكون حققنا شيء مهم وهو ضمان الحد الأدنى للصلاحيات والسماح بما نحتاج إليه فقط .

لكن هناك مشكلة كبيرة جداًا وهي موجودة في البروتوكولات نفسها , فبعض البروتوكولات لها طريقة خاصة في العمل , فمثلاً البروتوكولات العادية أوالطبيعية مثل الـ http»» أو telnet»» على سبيل المثال لهم بورت محدد ومعروف يمكننا على أساسه فلترته أو السماح به وهو 80 و 23 , حيث يُستخدم كـ destination port»» في أي packet»» ترسل إلى السيرفر , لكن بعض البروتوكولات الأخرى تقوم بإنشاء أكثر من session واحده,وتكون الـ session الاولى على بورت محدد ومعروف وفي أثناء هذه الـ session يتم الإتفاق على «»random port number آخر يتم بناء «»session ثانيه عليه , المشكلة في ذلك هو كيفيه تطبيق «الحد الأدنى للصلاحيات»؟ فإذا كنا نعرف البورت الذي يتم إنشاء الـ session الأولى عليه والسماح له بالمرور , فكيف نعرف البورت الثاني الذي يتم الاتفاق عليه في الـ session الأولى وهو رقم عشوائي وذلك لكي نقوم بالسماح له بالمرور ومن ثم نمنع أي شيء آخر؟ هذه هي المشكلة التي قد تضطرّنا إلى فتح «»range كبير من البورتات وذلك سيؤدي إلى Security Hole»» قد يتم استخدامها من قبل المخربين .

البروتوكولات التي تقوم بإنشاء أكثر من «»session معظمها يكون عبارة عن «Multimedia protocol» أو VOIP Protocol»» وبروتوكولات عامة أخرى مثل بروتوكول نقل الملفات FTP»» الذي هو محور حديثنا الآن .

كيف يعمل FTP Protocol ؟ :

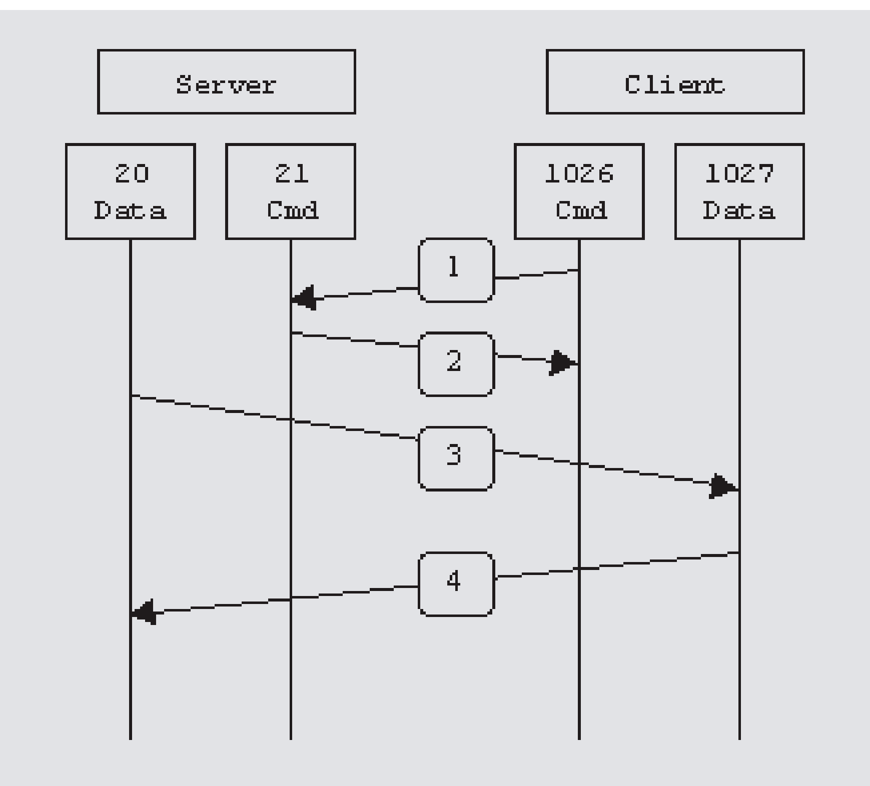
سؤال قد يبدو للبعض سخيفاً وسهل , والرد سيكون كالآتي - «يستخدم الـ TCP و يعمل هذا البورتوكول على بورت 21» ولكن في الحقيقة هذه الاجابة ليست كاملة وينقصها الكثير , الـ FTP يعمل على port 21 فعلاً , ولكن هذا البورت يسمى بـ command port أي يتم إرسال الأوامر إلى الـ FTP سيرفرعن طريق هذا البورت

لكن ماذا عن الـ data نفسها ؟هناك بورت آخرهو بورت 20 وهذا البورت خاص بالـ Data , الآن يكون عندنا 2 session , الأولى تكون الـ Destination port هو 21 والثانية هو 20 , وهنا يبدأ التعقيد , أحياناً لا يتم استخدام بورت 20 للـ data بل يتم استخدام رقم عشوائي , وهنا سنضطر إلى فتح«range» كبيرمن البورتات لكي ينجح هذا البروتوكول في العمل .

: FTP Modes

لهذا البروتوكول طريقتين في عمل«Modes» : الأول يسمى «»Active Mode والثاني يسمى Mode «Passive» , تعالوا نتعرف كيف يعمل هذا البروتوكول في كِلا الحالتين .

:FTP in Active Mode



في هذا الـ mode يقوم الـ client بالإتصال إلى السيرفرباستخدام port أكبرsource من 1023 , الـ command الـ يكون destination port port أي سيكون بورت 21 , بعد ذلك يقوم الـ server بانشاء«session » أخرى ويكون الـ port source من ناحية السيرفر 21 والـ destination port يساوي1+N , حرف N»» يمثل الـ source portالذي بدأ الـ Client الإتصال منه , الأمر يبدوا معقداً, لذا لنشرح على الصورة الآتية :

الخطوة الاولى1 step: يبدأ الـ client عملية الإتصال إلى السيرفر عن طريق source port يساوي 1026 والـ destination port يساوي 21 , في هذه الخطوة يقوم الـ client بإرسال أمر صغير و PORTوهو 1027 وعن طريق هذا الأمر يخبر السيرفر عن الـ destination port الذي سيستخدمه السيرفر لإنشاء «session» ثانية .

الخطوة الثانية2 step : يرسل السيرفر ACK على نفس الـ sessionليؤكد استلام المعلومات السابقة .

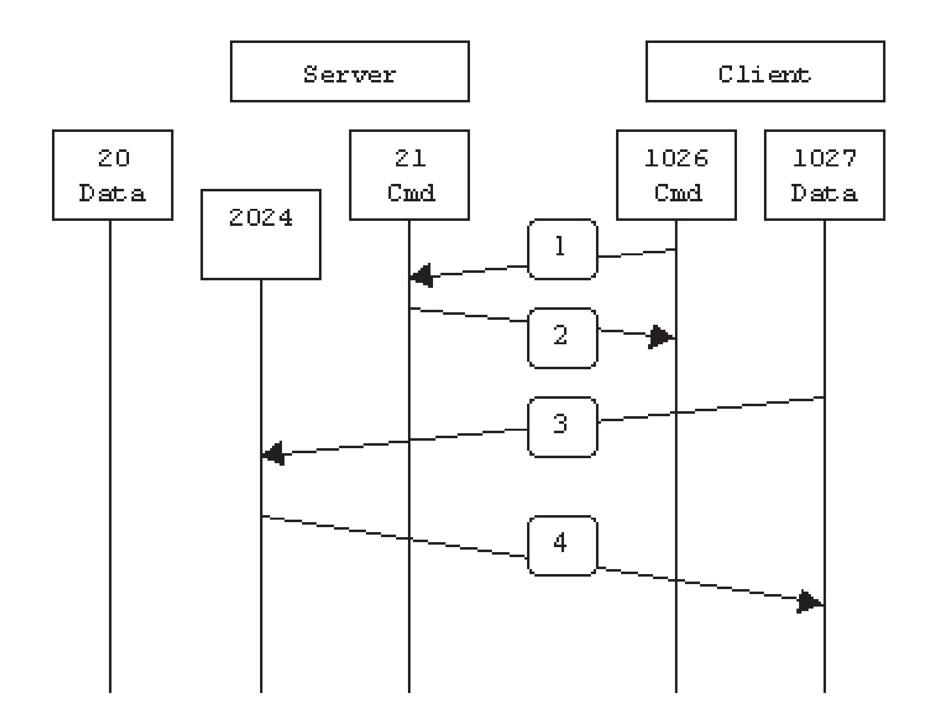
الخطوة الثالثة3 step : يبدأ السيرفر بإنشاء الـ SESSION الثانية التي سيكون الـ destination portلها هو 1027 الذي أرسله الـ clientفي step 1 .

الخطوة الرابعة4 step : يقوم الـ client بإرسال ACKليؤكد إنشاء الـ sessionالجديدة .

بهذا يكون عندنا اثنين «session» الاولى بين 1026 و 21 , وهذه الـ session يتم إرسال ما تحتويه من الأوامر فقط , الـ sessionالثانية بين 1027 و 20 وهي المسار الفعلي لـ data .

مشكلة الـ ACTIVE Modeهي في الخطوة رقم 3 , تخيّل معي أن لدينا مجموعة من الـ client خلف firewall»» ويحتاجون الوصول إلى ftp server»» موجود على الانترنت , ولإن الخطوة رقم ثلاثة يقوم بها السيرفرالذي يعتبره الـ firewall غيرموثوق أو «entrusted» لإنه يقع في الـ Outside, فسيقوم بمنع هذه الـ session لإنها تبدأ من الـ outsideودائماَ يقوم الـ firewall بمنع أي إتصال يبدأ من الـ outside , فمن تعامل مع أي «FIREWALL» من قبل سيفهم هذه الفكرة جيدا .





: FTP in Passive Mode

تم إنشاء هذا الـ Mode للتغلب على المشكلة السابقة التي كانت تحدث بسبب إبتداء السيرفر بإنشاء الـ «session» الثانية , تعالوا نتعرف على هذا الـ Modeلكي نرى الفرق بينه و بين الـ Active mode .

الخطوة الاولى1 step : يبدأ الـ client عملية الإتصال إلى السيرفر عن طريق « source port» والذي يساوي 1026 وعن طريق الـ destination portالذي يساوي 21 , في هذه الخطوة يقوم الـ client بإرسال أمر صغير وهو PASV وذلك بدلاً من الأمر Port في الـ Active mode .

الخطوة الثانية2 step : يقوم السيرفر بالرد و استخدام الأمر PORT 2024 ليحدد البورت الذي سيستخدمه الـ client في إنشاء الـ session الثانية , لاحظ هنا أنه تم عكس العملية التي تحدث في الـ active mode .

الخطوة الثالثة3 step : يقوم الـ client بعملية البدأ في إنشاء الـ data connection ويستخدم الـ destination port الذي استلمه فى step 2 .

الخطوة الرابعة4 step : يقوم السيرفر بإرسال ACK ليقوم بتأكيد إنشاء الـ session .

الـ passive mode قام بحل المشكلة السابقة التي كانت تحدث مع الـ Active mode ولكن في المقابل سبّبَ بحدوث مشكلتين إضافيتين , المشكلة الأولى : هي إذا كان عندنا «FTP server» وراء «firewall» وسمحنا لـ Clients الموجودين على الانترنت بالإتصال إلى هذا السيرفرسنضطرإلى فتح البورت 21 وrange كبير من البورتات التى قد يرسلها السيرفر إلى Clients في step 2 , أكرّر أنه لكي تفهم هذه المشكلة لا بد أن تكون لديك خلفية في طريقة التعامل مع الجدران النارية . المشكلة الثانية : هي أن هناك «FTP clients» لا تدعم الـ «FTP command line utility» المقدمة من «Solaris» , أما عندما تستخدم المتصفح كـ «FTP Client» فلن تواجهك أي مشكلة لإن معظم المتصفحات تدعم الـ PASV mode . بهذا أكون قد انتهيت من هذا المقال الذي أتمنى أن تكون استفدت منه ولو بكلمة واحدة .



شهادة شكر وتقدير

تتقدم إدارة موقع



بالشكر والتقدير للمهندس المصري

شريف مجدي

لكونه مثابر وإيجابي جدا على الصعيد الشخصي وعلى الصعيد العام
ولكونه ساهم معنا في كل المشاريع التى أطلقناها لخدمة المحتوى العربي الرقمي.

مؤسس ومدير موقع NetworkSet
المهندس أيمن النعيمي

2011 / 8 / 26



بعد أكثر من عشرين عاماً من العطاء بدأت تلوح على Cisco بعض مظاهر الخوف من ظهور وبروز أحد شركات المنافسة على الساحة العالمية والمعروفة بإسم Extreme ومما لا شك فيه أن هذه الشركة قادمة بقوة للمنافسة وخصوصاً في الشرق الأوسط .

وقبل أن نبدأ وحتى نكون عادلين يجب علينا أن نتفق على شيء واحد ومهم وهو يقول باختصار **لاتوجد شركة توصف بأنها الأفضل والأحسن** لأن الأمر قد يكون أحياناً معقد ومرتبط بوجود منتجات قد تكون مناسبة لك ولشركتك وغير مناسبة لشركة أخرى ولعدة أسباب مثل حجم الشبكة وميزانيتها وهل هي مرتبطة بشبكات LAN أو WAN أو وجود عقود مبرمة وتخفيضات والخ.....!

Cisco vs Extreme



على مستوى الـ Products

Cisco

سيسكو كما هو معروف عنها أنها المؤسس والحاكم لعالم اسمه الشبكات فهي تقدم منتجات وحلول لكل ماهو مرتبط بعالم الشبكات وهذا يشمل:
Routers, Switches, Wireless, Security, Voice, Video Conferencing, Data Center, Storage Network, Network Management, Interfaces and Modules, etc.....

Extreme

قد يكون تخصص هذه الشركة في قطاع السويتشات هو الذي جعلها تدخل سوق المنافسات في العالم , ولأن التخصص في مجال واحد يدفع دائماً إلى تقديم أفضل ما يكون وخصوصاً عندما يكون الإعتماد الرئيسي عليها وطبعاً هذا لم يمنع Extreme من الدخول في مجالات أخرى , لكن على مستوى بسيط ومحدود جداً لم يتعدى الجهازان في مجال الـ Security وخمسة أجهزة في مجال الـ Wireless بينما لا نجد أي منتجات خاصة بالروترات !.



على مستوى الـ Marketing

تحتل سيسكو المرتبة الأولى في العالم من ناحية المبيعات على الرغم من أنها الأكثر غلاء في الأسعار, ولكن نحن نعلم أن أسواق العالم بدأت تتغير في الآونة الأخيرة بسبب ظهور شركات بدأت تنافس فعلياً في السوق العالمية ومن بينها Juniper, Extreme, HP and Huawei. وبما أن المقارنة بين Cisco & Extreme فقد قمت بأختيار Series من كل شركة بحيث تكون متشابهة في الأداء والمواصفات ونفذّت المقارنة بينهم وفق مايلي :

Cisco 3750E-Series		
WS-C3750E-24TD-S	Catalyst 3750E 24 1010*2+1000/100/GE(X2),265W,IPB s/w	$9,495
WS-C3750E-24TD-E	Catalyst 3750E 24 1010*2+1000/100/GE(X2),265W,IPS s/w	$13,490
WS-C3750E-24TD-SD	Catalyst 3750E 24 10+ 1000/100/ 10*2GE(X2),265W DC, IPB s/w	$9,495
WS-C3750E-48TD-S	Catalyst 3750E 48 1010*2+1000/100/GE(X2),265W,IPB s/w	$18,995
WS-C3750E-48TD-E	Catalyst 3750E 48 1010*2+1000/100/GE(X2),265W,IPS s/w	$26,990
WS-C3750E-24PD-S	Catalyst 3750E 24 101000/100/ PoE+2*10GE(X2),750W,IPB s/w	$10,295
WS-C3750E-24PD-E	Catalyst 3750E 24 101000/100/ PoE+2*10GE(X2),750W,IPS s/w	$14,290
WS-C3750E-48PD-S	Catalyst 3750E 48 101000/100/ PoE+2*10GE(X2),750W,IPB s/w	$20,495
WS-C3750E-48PD-E	Catalyst 3750E 48 101000/100/ PoE+2*10GE(X2),750W,IPS s/w	$28,490
WS-C3750E-48PD-SF	Catalyst 3750E 48 101000/100/ PoE+2*10GE(X2),1150W,IPB s/w	$21,995
WS-C3750E-48PD-EF	Catalyst 3750E 48 101000/100/ PoE+2*10GE(X2),1150W,IPS s/w	$29,990
WS-C3750E-48TD-SD	Catalyst 3750E 48 10+ 1000/100/ 10*2GE(X2),265W DC, IPB s/w	$18,995

Extreme Summit X450a		
Summit X450a-24t	24 101000/100/BASE-T, 4 unpopulated 1000 base-X SFP (mini-GBIC) ports; dual 10G option slot, 2 dedicated 10G stacking ports, AC PSU, connector for EPS-500 or EPS-LD external redundant PSU, ExtremeXOS Advanced Edge license	$6,495.00
Summit X450a-24t Core License	ExtremeXOSTM Core License, SX450a-24t	$1,995.00
Summit X450a-24tDC	24 101000/100/BASE-T, 4 unpopulated 1000BASE-X SFP (mini-GBIC) ports; dual 10G option slot, 2 dedicated 10G stacking ports, DC PSU, connector for EPS-150DC external redundant PSU, XOS Advanced Edge license	$6,995.00
Summit X450a-24tDC Core License	ExtremeXOSTM Core License, SX450a-24tDC	$1,995.00
Summit X450a-24x	24 1000BASE-X mini-GBIC ports, 4 101000/100/BASE-T ports,option slot for 10 Gigabit option card XGM22-xn/xf, 1 AC PSU, ExtremeXOSTM Advanced Edge license, connector for EPS-500 or EPS-LD external redundant PSU	$8,995.00
Summit X450a-24x Core License	ExtremeXOSTM Core License, SX450a-24x	$1,995.00
Summit X450a-48t	48 101000/100/BASE-T, 4 unpopulated 1000BASE-X SFP (mini-GBIC) ports; dual 10G option slot, 2 dedicated 10G stacking ports, connector for EPS-500 external redundant PSU, ExtremeXOS Advanced Edge license	$8,995.00
Summit X450a-48t Core License	ExtremeXOSTM Core License, SX450a-48t	$1,995.00
Summit X450a-24xDC	24 1000BASE-X mini-GBIC, 4 101000/100/BASE-T ports, option slot for 10 Gigabit option card XGM22-xn/xf, 1 DC PSU,ExtremeXOSTM Advanced Edge license, connector for EPS-150DC external redundant PSU	$9,495.00
Summit X450a-24xDC Core License	ExtremeXOSTM Core License, SX450a-24xDC	$1,995.00
Summit X450a-48tDC	48 101000/100/BASE-T, 4 unpopulated mini-GBIC ports, option slot for 10 Gigabit option card XGM22-xn/xf, 1 DC PSU, ExtremeXOSTM Advanced Edge license, connector for EPS-150DC external redundant PSU	$9,495.00
Summit X450a-48tDC Core License	ExtremeXOSTM Core License, SX450a-48tDC	$ 1.995.00

ملاحظة هامة : الأسعار غير دقيقة وقد تم الاعتماد على بعض المواقع المشهورة للحصول عليها, وهي كحال أي جهاز تقني سعره يتغير بشكل مستمر كلما ظهر شيئ أحدث وأفضل



مخطط يشير إلى أرتفاع معدلات البيع الخاصة بأجهزة إكستريم إبتدا من عام 2007 إلى نهاية 2009

Extreme Increasing CESR Market Share
CESR = Carrier Ethernet Switch Router

Extreme CESR Market Share

Rolling 4 Quarter Market Share %

3Q07	4Q07	1Q08	2Q08	3Q08	4Q08	1Q09
2.5%	2.6%	3.0%	3.5%	4.0%	4.5%	5.4%

•Source: Heavy Reading Research, CESR Quarterly Tracker, July 2009

Growing Worldwide Carrier Ethernet Switch Router Market Share as Global Economy Stalls

على مستوى نظام التشغيل

Cisco

IOS: لإكثر من عشرين عام كان هذا النظام هو الرقم واحد في عالم الشبكات من حيث الاستخدام ومازال , وهو يُعدّ Monolithic Operating System وترجمته تعني أنه نظام متكامل ومتناغم , ومعنى هذا الكلام يعود إلى أن نظام سيسكو عندما يعمل فإنه يكون كقطعة واحدة تتشارك فيه كل العمليات في نفس الحيّز من الذاكرة RAM , وبسبب هذا التشارك في الذاكرة وعدم وجود حماية بين العمليات التي تجري على الذاكرة يؤدي هذا أحياناً إلى حدوث خلل في جميع العمليات وفقد بعض المعلومات في حال كان هناك أي خطأ برمجي في أي عملية على الذاكرة , وبمحاولة من سيسكو لتفادي هذه المشكلة أعلنت عن

```
C3640-jk9s-mz.12416-a.bin
C7200-adventerprisek9-mz.1244-.T1.bin
```

إصدار جيلٍ جديد من الـ IOS تحت اسم IOS XR معتمداً على Third party System يدعى QNX لتنصيب نظامها الجديد و الذي يعمل في أجهزة CRS العملاقة والذي يعدModular operating system المشابه لنظام Extreme بالإضافة إلى وجود نوعين آخرين يحملان الأسماء التالية : IOS XE, NX-OS

وتصدر سيسكو نظام IOS مخصص لكل جهاز من أجهزته يحمل رقم الـ Series الذي يتبعه مثلا :

وآخر إصدار من IOS كان يحمل الرقم 15.0 وتحتاج عملية تحديث النظام بشكل عام إلى إزالة النظام القديم بشكل كامل ووضع النظام الجديد في مكانه , بالإضافة إلى اختلاف طريقة كتابة الأوامر أحياناً من نسخة لأخرى , كما يتطلب تنفيذ شيء معيّن , كتابة أكثر من سطر في موجه الأوامر كما سوف نشاهد فيما بعد .

Extreme

في Extreme هناك نظامان للتشغيل فقط , وبعكس سيسكو التي تعتمد نظام تشغيل لكل جهاز لديها «(روتر,سويتش,جدار ناري)» كما شاهدنا سابقاً.

أما الأنظمة في Extreme فهي تعد Modular operating system تم إعداده لكي يعمل على نظام تشغيل مفتوح المصدر يُعرف بـ FreeBSD , وبالتالي هذا يؤمن للعمليات التي تجري الخصوصية والحماية من خلال توفير مساحة خاصة من الذاكرة RAM لكل عملية , بالإضافة إلى إمكانية تحديث النظام أو إضافة Feature جديدة في أي وقت ومن دون الحاجة إلى إزالة نظام التشغيل أو حتى إعادة تشغيله , ولهذا النظام نوعان كما ذكرنا وهم :

Extreme Ware: وهو نظام محدود مقارنة مع النظام الآخر وهو يعمل على الأجهزة البسيطة من Extreme ويدعم بعض بروتوكولات الطبقة الثانية والثالثة والتي سوف نطّلع عليها بعد قليل, ويميزه بساطة وسهولة تنفيذ الإعدادات, وقد توقف التعامل معه تقريبا.

Extreme XOS: وهو نظام مطور ويدعم خواص



كثيرة جداً تجعله النظام الأول لأغلب أجهزة Extreme فهو يدعم كل ما هو موجود على أنظمة Extreme Ware بالأضافة إلى high-availability architecture, extensibility via XML, dynamic application loading, and Universal Port Scripting.

وهــــذا جــدول يوضح أهـــم الفروقـــات بين النظامين :

ExtremeWare and ExtremeXOS	ExtremeXOS
• Network login • IP security • Hitless failover/upgrade • MAC security • Host integrity checking integration • LLDP • SNMPv1/v2/v3 • SSH2/SCP • EAPS, STP, ESRP, VRRP • OSPF, RIP, BGP • PIM • sFlow (i-series platforms)	• IPv6 Layer 2 Layer 3 support • Process monitoring and restart • Process memory protection • XML APIs • Dynamic software module loading • CLI scripting • Universal Port • Virtual routers • CLEAR-Flow

على مستوى طريقة كتابة أوامر Cisco & Extreme

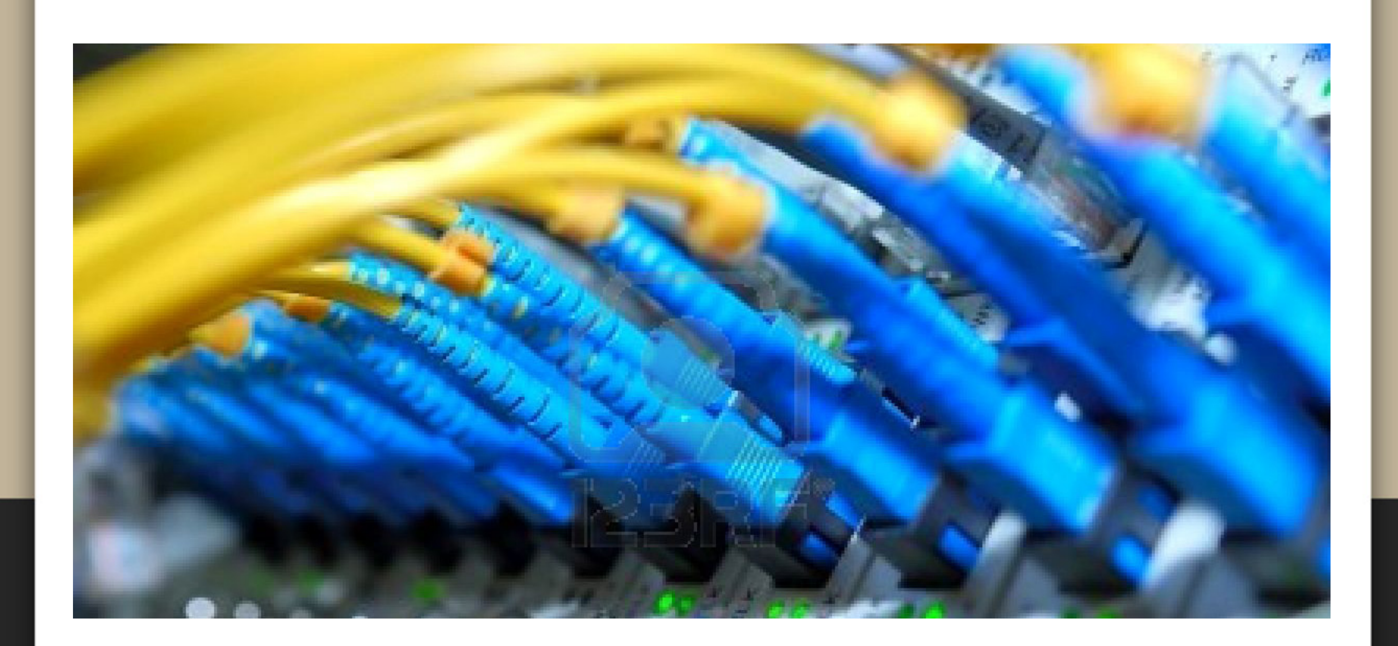
Cisco (IOS)	Extreme (XOS)
hostname NetworkSet	configure snmp sysname NetworkSet
vlan database vlan 2 name mgmt exit	create vlan mgmt configure vlan mgmt tag 2
interface vlan mgmt ip address 192.168.1.1 255.255.255.0 no shutdown	configure vlan mgmt ipaddress 192.168.1.1 /24
interface g04/ switchport mode access switchport access vlan 2	configure vlan mgmt add port 4 tagged
write memory	save
show interface g04/ show ip route show cdp neighbors show vlan show mac-address-table show run	show port 4 information detail show iproute show edp port all show vlan show fdb show config

خلاصة هذا الكلام : أجهزة سيسكو سوف تبقى الرقم واحد عالمياً رغم كلفتها العالية , ولسبب واحد وهام وهو «رأي شخصي» وهو الدعم الفني Support الذي حرصت عليه منذ بدايات دخولها عالم الشبكات , فلو حدثت مشكلة ما في أحد أجهزتها فيكفي الدخول إلى أحد محركات البحث «غوغل» مثلاً وسوف تجد آلاف المواقع التي تتحدث عن مثل هذه المشاكل , ولو في حال لم تجد حل للمشكلة !! يمكنك ببساطة التواصل مع الدعم الخاص بشركة سيسكو وسوف يكونوا سعداء جداً لمساعدتك وحل مشكلتك بسرعة فائقة , بالإضافة إلى وجود عدد كبير جداً من الفنيين والمهندسين الحاصلين على شهادات إحترافية في سيسكو, بينما من الصعب إيجاد خبير في أجهزة Extreme , لإنه يتطلب حضور دورات تدريبية تقوم بها الشركة في بعض مراكزها المنتشرة في العالم.

لكن من طرف آخر نجد أن عالم الشبكات أصبح يدار أغلبه من خلال أجهزة السويتش المتعددة الإستخدامات (Layer2, Layer3, Multi Layer Switch) والذي سوف نجده في أجهزة Extreme فهي تركز على هذا النوع من الاجهزة وأعتمدته لكي يكون المنتج الأساسي لها , لذا سوف نجده الأفضل في مجاله من حيث الأداء العالي والسعر الأفضل , فلو أطّلعنا على قائمة الأسعار سوف نجد أن أرخص سويتش من سيسكو يدعم تقنية الـ Power Over Ethernet يصل سعره إلى «عشرة آلاف دولار» بينما نجد أن أسعار أجهزة Extreme يصل سعرها إلى «سبعة آلاف دولار» أي أرخص بنسبة «ثلاثين بالمئة» من منافستها سيسكو وهذه العملية الحسابية توصلنا إلى نقطة مهمة يجب أخذها بعين الإعتبار , وأخيراً سمعة الشركة في الأسواق جيدة ولا غبار عليها حتى الآن.









شبكات سيسكو اللاسلكية

لمحة عن الكاتب
أمجد عبد الله
الجنسية : الأردن
مهندس شبكات لاسلكيّة في مركز الدعم الفني في سيسكو - Cisco TechnicalAssistance Center (TAC)
andalus_pc@hotmail.com

تعتبر تكنلوجيا الاتّصالات اللاسلكيّة من أهمّ التكنلوجيا المستخدمة حالياً , ويعود الفضل في إشعال فتيل الثّورة اللاسلكية إلى العالم الاسكوتلندي «جيمس كلارك ماكسويل» , الذي اكتشف وفسرّ سلوك الموجات اللاسلكيّة بمعادلاته المعروفة .

هناك شركات كثيرة مساهمة ومعروفة في مجال تكنلوجيا الاتّصالات اللاسلكيّة الخاصّة و المستخدمة لأغراض ربط الشّبكات , ومن أهمّ هذه الشّركات : Aruba وMotorolla و Cisco.

دخلت شركة سيسكو معترك الشبكات اللاسلكية بشكل أساسي بعد شراءها لشركة Aironet عام 1999 , ثمّ بدأت تطوّر المنتجات من ناحية النّوع والخصائص شيئاً فشيئاً إلى أن وصلت إلى ما هي عليه الآن .

وفي هذا المقالة سنستعرض بشكل موجز بعضاً من المُنتجات الرئيسيّة التي تستخدم في الشّبكات اللاسلكيّة لسيسكو ووظيفة كلّ منها :

-1) نقاط الاتّصال (Access Points): تعتبر نقاط الاتّصال من أهمّ ما يشكّل الشّبكة اللاسلكيّة , وربّما هي أوّل ما يخطر ببال الشّخص عند ذكر الشّبكات اللاسلكيّة. نقاط الاتّصال هي رابط يربط ما بين الشّبكة اللاسلكيّة والشّبكة السلكيّة. فلها موصل راديوي (radio interface) وموصل سلكي (XEthernet Interface) . يتّصل المستخدمون للشبكة اللاسلكيّة مع نقاط الاتّصال عن طريق الموصل الراديوي ثمّ تقوم نقطة الاتّصال بإرسال الإشارات إلى الشّبكة السلكيّة عن طريق المنفذ السّلكي .

هناك نوعان رئيسيّان من نقاط الاتّصال :

i) نقاط اتّصال مستقلّة (autonomous or standalone APs): وهي نقاط الاتّصال التي تقوم بخدمة مستخدمي الشّبكة اللاسلكيّة بشكل مستقل دون الحاجة أو المعونة من أيّ أطراف أخرى.

ii) نقاط اتّصال متّحدة (خفيفة الحِمل) (Unified or lightweight APs): وهي نقاط اتّصال تقوم بتقديم الخدمة اللاسلكيّة للمستخدمين بشكل جزئي ويكمّل الجزء الآخر جهاز آخر يجب أن تتّصل معه نقطة الاتّصال وتكون متلائمة معه ويسمّى هذا الجهاز المُتحكِّم (controller).

نقاط اتصال لاسلكيّة (Access Points) بأشكال وموديلات مختلفة:







-) متحكمات الشّبكة اللاسلكيّة (Wireless LAN Controllers - WLCs): ويعتبر هذا هو الجهاز المركزي أو العقل المُدبّر للشّبكات اللاسلكيّة المُتّحدة (unified) , والتي تكون فيها نقاط الاتّصال مربوطة بالمُتحكّم , وهو يقوم بإعطاء الأوامر لنقاط الاتّصال لتقوم بعملها. نقاط الاتّصال المستقلّة لا تحتاج إلى متحكّم وتقوم بالعمل بشكل مستقل. فائدة وجود مُتحكّم هي أنّه يمكنك التّحكم بعدد كبير من نقاط الاتّصال بيسر وسهولة من مكان مركزي , وبالقيام بالأمر مرّة واحدة فقط وتطبيقه على أكثر من نقطة اتّصال. بينما في حال نقاط الاتّصال المستقلّة فإنّه وعند وجود عدد كبير من نقاط الاتّصال يجب أن يتمّ عليها تعديل فإنّه يتوجّب عمل التّعديل على كل نقطة بشكل مستقل ممّا يستهلك وقتاً وجهداً.

صور لبعض أنواع المتحكمات (Wireless LAN Controllers):

متحكم سيسكو موديل 2100



متحكّم سيسكو مدمج. يتم تركيبه كـ module على بعض أنواع الراوترات:

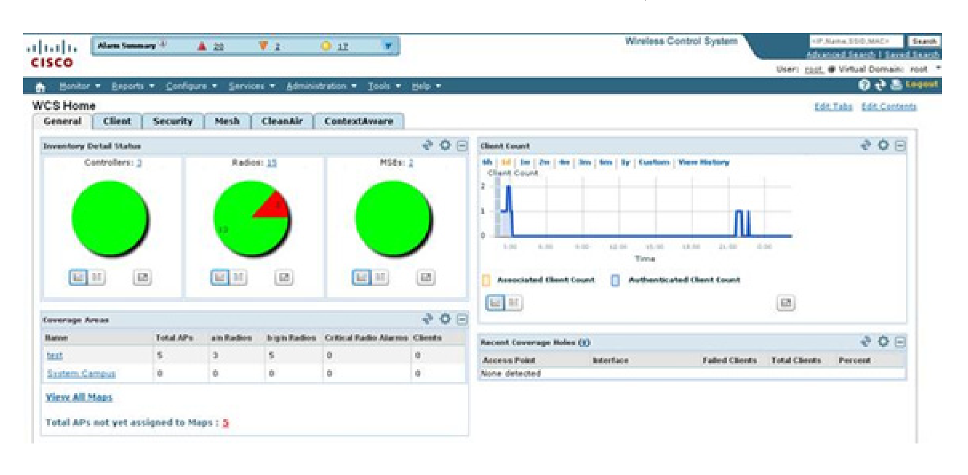


-3) الجسور اللاسلكيّة (bridges): وهي شبيهة بنقاط الاتّصال , لكنّ الفرق في أنّ الهدف الأساسي منها هو ليس تقديم خدمة الاتّصال للمستخدمين العاديين , بل الهدف منها هو وصل شبكتين سلكيتين تفصل بينهما مسافة معيّنة بواسطة شبكة لاسلكيّة. فيوضع جسر لاسلكي على طرف كل من الشبكتين السلكيتين المطلوب وصلهما ويتم توجيه الجسرين بحيث يكونا متقابلين,عندها يمكن للشبكتين السلكيّتين الاتّصال مع بعضهما البعض عن طريق الشّبكة اللاسلكيّة .

صورلبعض الجسوراللاسلكيّة بأشكال وموديلات مختلفة:



الواجهة الرسوميّة لنظام إدارة الشّبكة اللاسلكيّة من سيسكو Wireless Control System

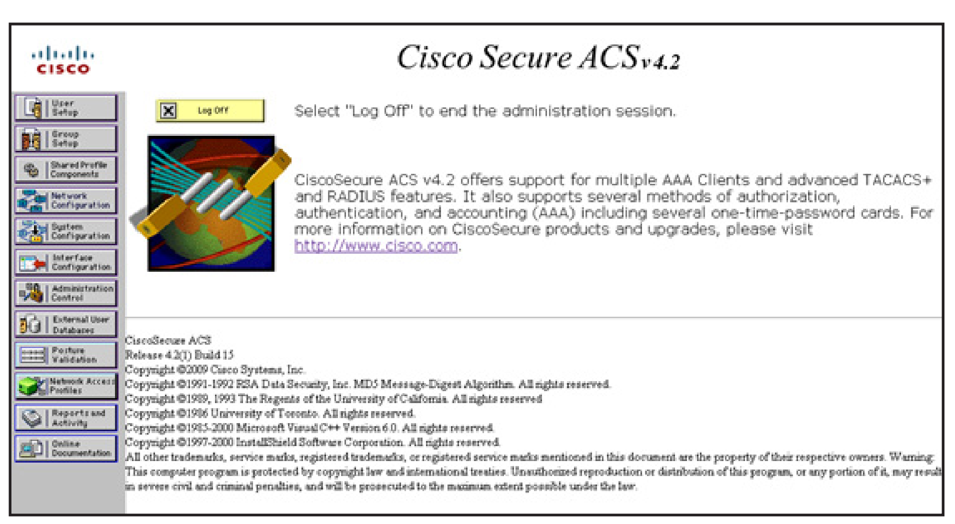


4- أنظمة إدارة الشبكة اللاسلكيّة (Wireless Management Systems):
ومن الأمثلة عليها منتج سيسكو المُسمّى Wireless Control System WCS - والهدف منها هو مراقبة الشّبكة اللاسلكيّة وتقديم معلومات عامّة عنها , مثل : عدد المستخدمين الموجودين، حالة الشّبكة اللاسلكيّة وإذا كان هناك أيّ مشاكل، ربط الشّبكة اللاسلكيّة بخدمات أخرى (مثل الخرائط وأنظمة مراقبة الموقع - Location services). كما يكون نظام إدارة الشّبكة اللاسلكيّة ذا أهميّة كبيرة في حال وجود عدد كبيرٍ من المتحكمات (Controllers) بحيث يصعب متابعة كل واحد على حدة. فيقوم نظام الإدارة هذا بمراقبة جميع المُتحكّمات وعرض ما عليها من نقاط اتّصال ومستخدمين متّصلين وإعطاء تفصيل عن حالة كل جزء من الشّبكة وكذلك إعطاء تقرير عن حالة الشّبكة خلال مدّة معيّنة .



5- Location Systems: ومن الأمثلة عليها في سيسكو ما يُعرف بـ Mobility Services Engine والذي يقوم عند ربطه مع WCS بإعطاء تقرير عن مواقع المستخدمين المرتبطين بالشّبكة. ويجب قبل ربطه بـ WCS وضع خارطة توضّح الأماكن المغطاة بالشبكة اللاسلكيّة ويتم وضع أماكن نقاط الاتّصال على هذه الشّبكة. عندما يقوم الـ MSE بعمل حسابات تقوم بإظهار موقع تقريبي لموقع المستخدمين اللاسلكيّن على الخارطة. وليقوم الـ MSE بعمله على أتمّ وجه يجب مراعاة تصميم وضع نقاط الاتّصال بشكل يتلائم مع حسابات الـ MSE لإعطاء أفضل دقّة ممكنة عند تحديد مواقع المستخدمين .

6- خادمات الحماية - Security Servers: ومن الأمثلة عليها Radius Server و TACACS+ Server والتي يتم ربطها عادةً بالشّبكة اللاسلكيّة كقاعدة بيانات للمستخدمين المخوّلين بالدّخول على الشّبكة. فيتم ضبط الشّبكة اللاسلكيّة لاستخدام أحد خادمات الحماية , وعند محاولة أحد المستخدمين الدخول للشّبكة اللاسلكيّة فإنّ الجهاز اللاسلكي (نقطة الاتّصال في حالة الشبكات المستقلّة أو المُتحكّم في حال الشبكات الموحّدة) يقوم بإرسال طلب الاتّصال إلى خادم الحماية ليقوم بدوره بالتقرير عما إذا كان هذا المستخدم مسموحاً له بالدّخول إلى الشّبكة أم لا. تسمّى هذه العمليّة بعمليّة تأكيد الهويّة - authentication.



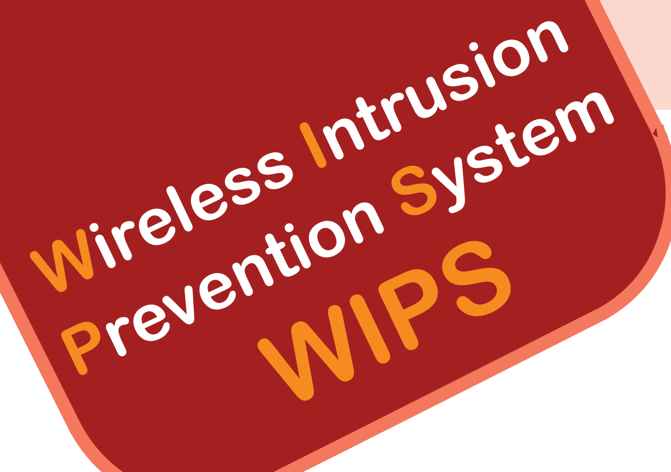
الواجهة الرّسوميّة لـ ACS server الإصدار 4.2(1)

-7) الهوائيّات - antennas: وهي عبارة عن أجهزة يتم ربطها بنقاط الاتّصال أو الجسور اللاسلكيّة لتقوم ببثّ الإشارة اللاسلكيّة. والهوائيّات هي شيء أساسي إذ بدونها لا يمكن نشر الشبكة اللاسلكيّة في المحيط. بعض الهوائيّات تكون مُدمجة مع نقاط الاتّصال أو الجسور اللاسلكيّة بينما يكون بعضها الآخر خارجيّاً ويمكن توصيله بنقطة الاتّصال أو الجهاز اللاسلكي عن طريق كابل توصيل. تختلف الهوائيّات من حيث قوّة الإشارة التي تبثّها، ففيمَ تقوم بعض الهوائيّات ببث الإشارة إلى عشرات الأمتار فقط فإنّ بعضها قد يبثّ الإشارة إلى مئات أو ربّما آلاف الأمتار .

أشكال مختلفة لبعض الهوائيات:



أتمنّى أن يكون هذا العرض البسيط مفيداً. ونلتقي إن شاء اللّه في مقالات أخرى لشرح بعض ما عرضناه هنا بشكل أكثر تفصيلاً.







من المعروف أن الشبكات اللاسلكية من أكثر الشبكات تعرضاً للإختراق , ومن الممكن إختراقها بسهولة نوعاً ما , وذلك بسبب انتشار تردداتها وعدم تقيدها في مجال معين , لذا وُجدت أنظمة منع إختراقات الشبكة اللاسلكية .

ماهو نظام WIPS:-

هو جهاز شبكة يراقب الترددات أو الطيف الترددي ويراقب الترددات ونقاط الوصول الغير مصرح لها عن طريق كشف التسلل ويمكن لهذا الجهاز أخذ تدابير مضادة (تلقائيا) منع التسلل .

اغراض WIPS:-

الغرض الأساسي من أجهزة منع إختراق الشبكة اللاسلكية هو منع الوصول الغير المصرح به إلى الشبكات المحلية وغيرها من معلومات الأجهزة اللاسلكية , وهذه الأجهزة عادةً ما تكون مضافة أو مدمجة إلى البنية التركيبية للشبكة المحلية اللاسلكية.

كشف التسلل (كشف التسلل Intrusion detection):-

نظام لاسلكي يراقب الترددات والأطياف الترددية للأجهزة ونقاط الوصول الغير مصرح بها , ويعمل على تنبيه مدير النظام على الفور , ويتم ذلك عن طريق مقارنة عناوين الماك أدرس من الأجهزة المشتركة والمسجلة في النظام , ولكن مع التطور وتطور العابثين فمن الممكن عمل تزوير أو تزيف للماك أدرس , ويقوم الباحثين على تطوير عملية كشف التسلل بعمل
أسلوب تقفّي الأثر للأجهزة التي تعمل spoof MAC . ومقارنتها بنمط آخر من التردد يطلق عليها التوقيع . بنمط مسجل للجهاز المصرح به داخل الشبكة

(منع التسلل Intrusion prevention):-

ويضاف إلى أجهزة منع إختراق الأنظمة اللاسلكية نظام منع التسلل كمرحلة ثانية بعد كشف التسلل , وهي قادرة على الكشف بدقة لترددات وتصنيفها تلقائياً حسب التهديدات , ويمكن الوقاية من التهديدات التالية عن طريق أنظمة منع اختراقات الشبكة اللاسلكية :

التكوين الخاطىء لإعدادات نقطة الوصول	Mis-configured AP
هجمات الرجل في الوسط	Man in the Middle Attack
تزوير أو تزييف الماك أدرس	Mac-Spoofing
أوعية العسل وهجمات توأم الشر	Honey pot / Evil Twin Attack
هجمات حجب الخدمة أو نكران الخدمة	Denial of Service (DoS) Attack

مكونات WIPS:-

أجهزة الاستشعار : وتحتوي على أجهزة استقبال و أجهزة لبث الموجات لفحص طيف الشبكة اللاسلكية .

الخادم :- خادم مركزي لنظام منع الإختراقات اللاسلكية , ووظيفة هذا الخادم هي تحليل الموجات الملتقطة بواسطة أجهزة الاستشعار .

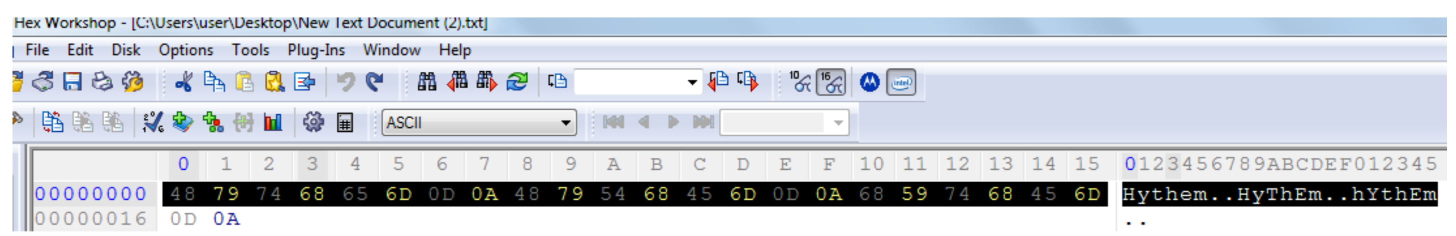
والكونسول:- واجهة رسومية للجهاز ويستخدمها المدير لإدارة التقارير .



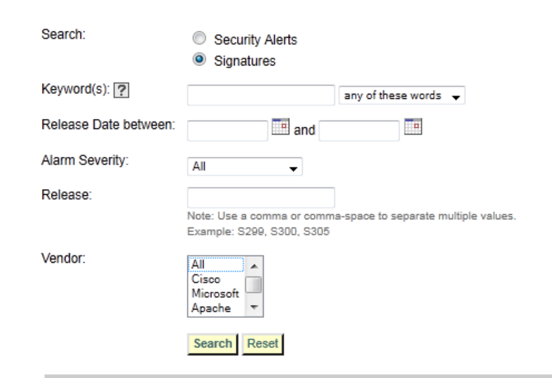
:-IPS signature

التوقيع الرقمي : وهو عبار عن مجموعة القواعد المخزنة على شكل بيانات في داتا بيز قريب جداً بعمل المضاد للفيروسات لاستشعار الباكيت المار في الشبكة وتحليلها مثلئ هجمات حجب الخدمة والفلود ....الخ sensor ويستخدم الحساس أو المستشعر

ولكن كيف يعمل التوقيع بالضبط ؟ سوف اقرب الصورة لك أخي القارىء .
عندما تمر البيانات أو الموجات الترددية الطيفية يقوم الحساس بمقارنتها بما لديه من معلومات مخزنة في قواعد و وتكون البيانات مخزنة على شكل ست عشري hythem البيانات , دعونا نأخذ مثال واقعي أريد مراقبة الباكيت بكلمة
وعن مقارنة الباكيت بكلمة هيثم ووجودها من ضمن التوقيع المحظور سوف يعمل النظام بتجاهل للباكيت وحذفها من HyTheM الرزمة المارة في الشبكة اها كلام جميل طيب ولكن اذا حصل تلاعب في الباكيت وحقن كلمة سوف تعبر الباكيت بكل سهولة لنا ليست موجودة في البيانات المخزنة فما العمل؟ . لقد قام الباحثون على تطوير والعمل على هذه النقطة واخذ جميع الاحتمالات لتفادي مثل هذه الامور .



ويتم احضار هذا التواقع حسب الجهاز المستعمل وهذه صورة من موقع سيسكو



خطوات لحماية شبكتك اللاسلكية :-

لقد تكلمنا عن جهاز حماية الشبكات اللاسلكية من الإختراق , ولكن يجب على كل شخص منّا توفير الحماية لشبكته بالطرق التقليدية والتي لا تحتاج أجهزة مكلفة للمستخدم العادي , ويمكن تلخيص هذه النقاط كالتالي :

1- تغير الباسورد الافتراضي للمدير إلى أن يأتي في إعداد المودم .

2- وتغيير اسم الشبكة .SSIDايقا ف عملية البث في اسم الشبكة اللاسلكية التقليل من الاشارة اللاسلكية ووضع المودم في وسط المنزل, وإبعاده عن النافدة للتقيل من وصول المتطفلين

3 - التأكد من تحديث برامج جهازك بشكل دوري ومتصفح الإنترنت والتإكد من أن الفيرول لنظام التشغيل ليس مغلق وتحديث البرامج المضادة للفيروسات .

4- استخدام تشفير قوي مثل WAP, WAP2

5- تذكر ان تشفير WEB أفضل من وضع المود بدون تشفير

6 - استخدام الفلترة للماك أدرس ووضع الماك أدرس للستخدمين المخول لهم في الشبكة .

7 - ايقاف خاصية الإتصال عن بعد واستخدام الاتصال بالمودم عن طريق سلك الشبكة



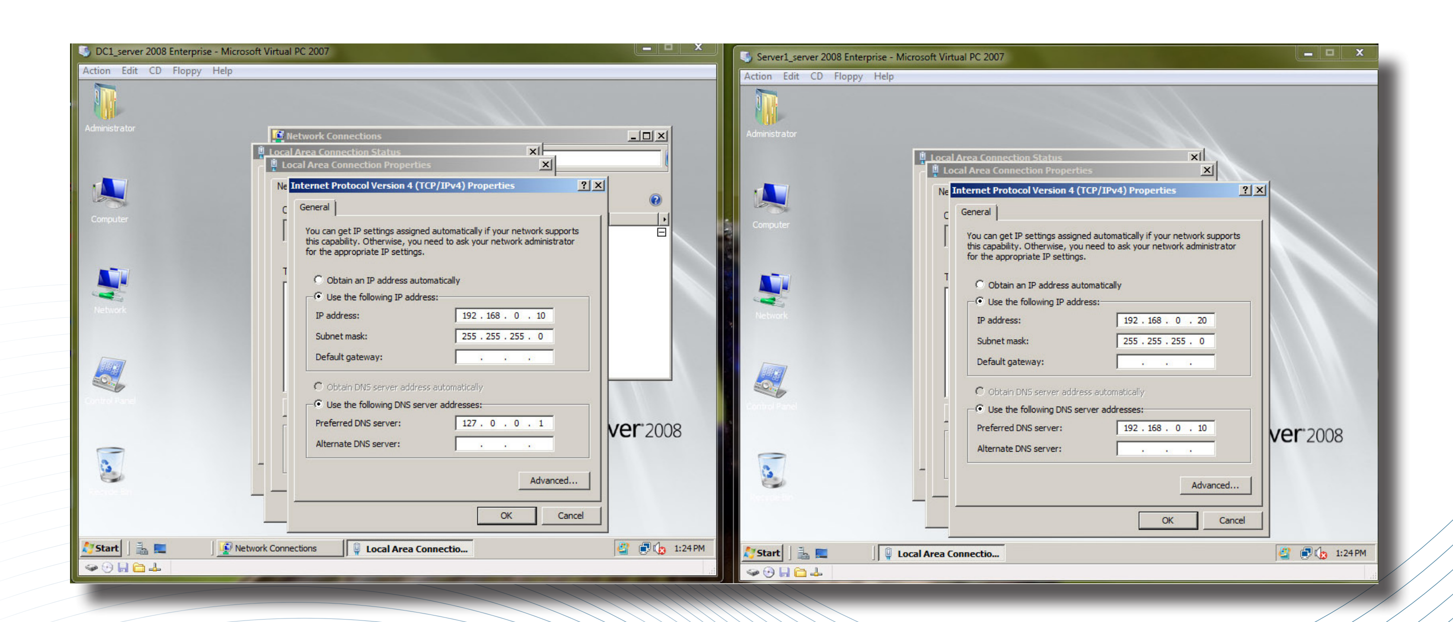
كيفية ربط الفروع بواسطة خاصية RODC

في عالم الأعمال و في ظل التوسع التكنولوجي الذي نشاهده في الوقت الحاضر , نشاهد شركات تسعى إلى توسيع رقعة العمل التي تحتلها في السوق و الانتقال إلى بيئات عمل أخرى مع الحفاظ على طبيعة و كينونة العمل التي تختص بها .

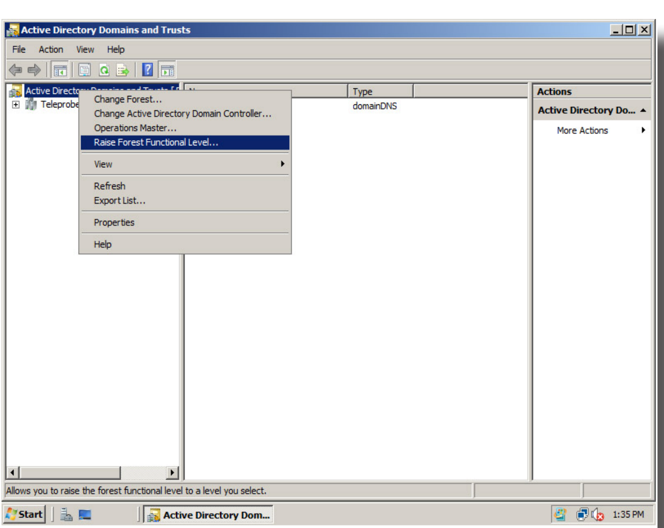
دائماً عندما نشاهد أو نسمع عن شركة قد تم افتتاحها في دولة أو في محافظة ما , ربما نتساءل عن كيفية ربط و تنسيق العمل مع هذه الفروع ؟ . و من طرق الربط التي قد نستفيد منها هي : وجود أكثر من سيرفر و يحملوا نفس اسم الـDomain Controller و لكن بصلاحيات أقل , حيث يمكن أن تمنح الصلاحيات إلى موظف آخر غير الـSystem Administrator .

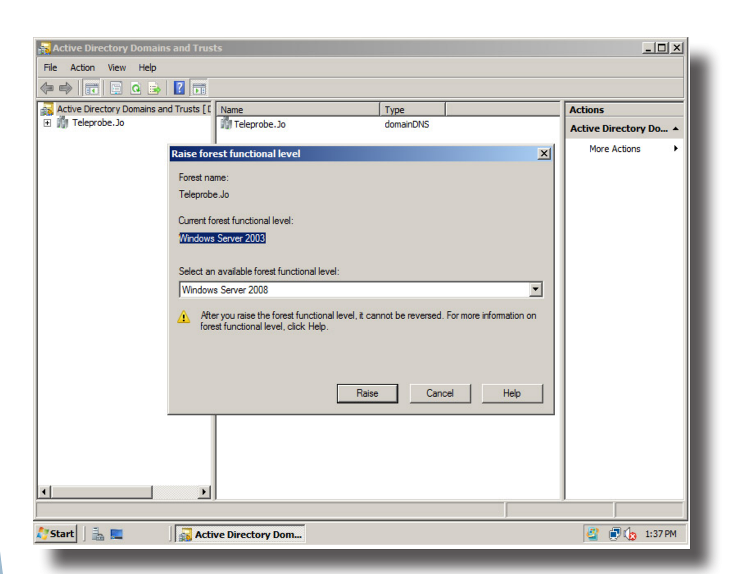
طريقة الـRODC« Read Only Domain Controller» , سوف يتم عرض هذه الطريقة التي أوجدتها مايكروسوفت حديثاً في نسخة السيرفر 2008 والتي لم تكن موجودة في السيرفر 2003 , و ذلك للتخفيف من الـtraffic في حالة الفروع في الشركات أو ما شابه ذلك ، وهو أيضاً يصنف على أن يكون دومين إضافي ولكن يكون للقراءة فقط و لا يمكن إضافة أو تعديل اسم حساب في قائمة الـ Active Directory.

طبعاً طريقة الـ RODC يجب أن يكون لديك سيرفرين , الأول الذي يوجد عليه الـDomain Controller , و الثاني الذي سوف يوضع في الفرع الأخر , و في خطواتنا التالية سوف يكون لدينا سيرفرين الـ DC و يحمل الـ IP 192.168.0.10 , و سيرفر آخر سوف يكون عليه الـ IP 192.168.0.20 ، و يحمل اسم Server2.



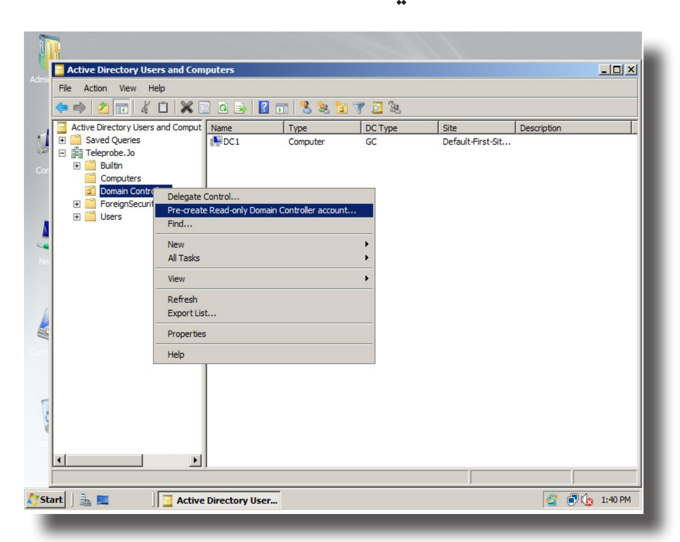
من أهم الخطوات التي يجب عملها لتجنب حدوث أي مشكلة في حالة التجهيز لـ RODC هو عمل الـFunctional Level من Active Directory Domains and Trusts إلى windows server 2003 حتى تكون عملية التحويل إلى RODC من دون أي مشاكل. و نعمل هذه الطريقة في الـ DC الرئيسي.

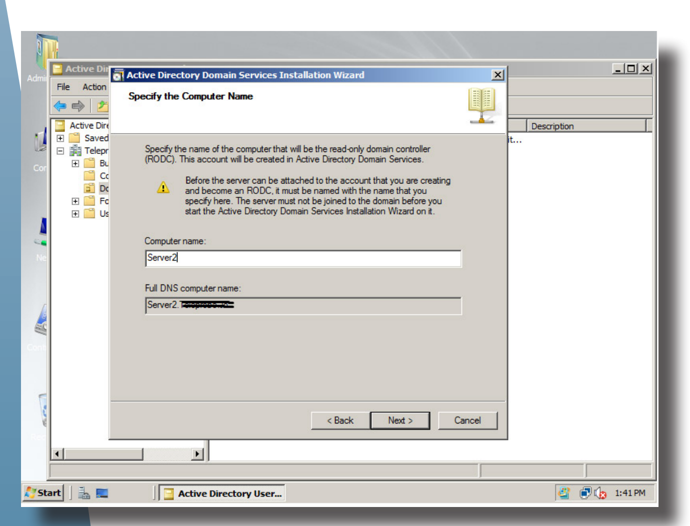




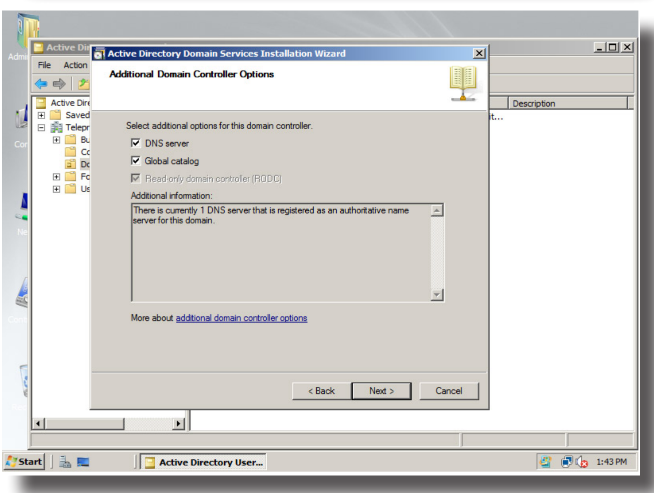
و من ثم نذهب إلى الـ Active Directory Users and Computers ونقوم بحجز مكان للجهاز و ذلك عن طريق الخيار Pre-create Domain Controller Account و تظهر لنا شاشة يتم فيها إضافة اسم السيرفر الذي تريد عمل الـ RODC عليه .

و للتأكد من أننا في الطريق الصحيح سوف يظهر لنا خيار الـ RODC يوجد عليه Checked و لكن لم أتمكن من التعديل عليه في هذه الصورة .



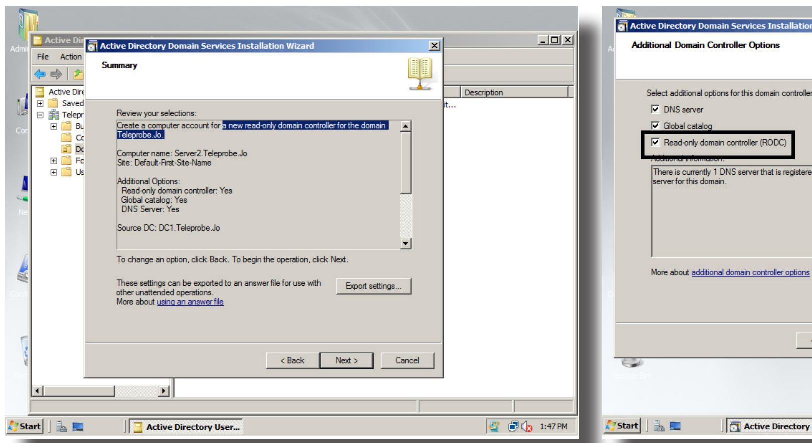


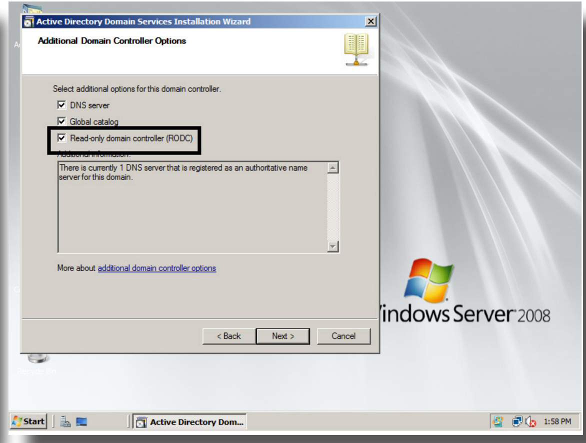
و من الإضافات المميزة أنّه يمكن عمل مجموعة خاصة أو Group , و يكون من صلاحياتها فقط الدخول إلى السيرفر , الـ RODC يمكن تركها فارغة و التعديل عليها لاحقاً.



بعد ذلك نذهب إلى السيرفر الـServer2 و نكتب الأمر Dcpromo في الـ RUN و نتبع الأوامر التالية :

Dcpromo>>Existing forest>>add a domain Controller in An existing Domain



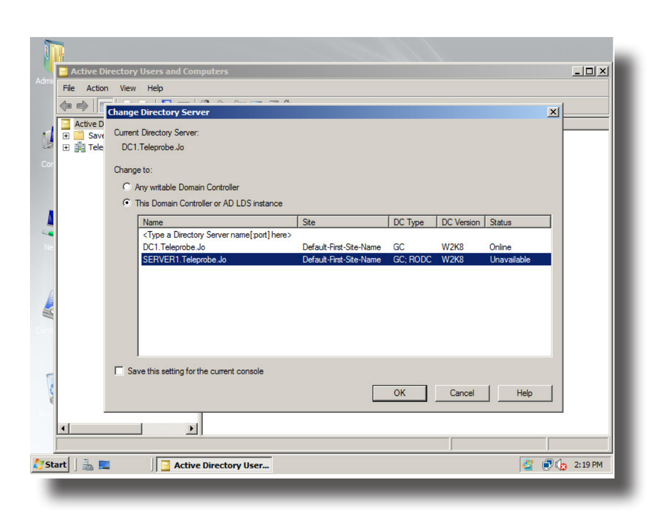


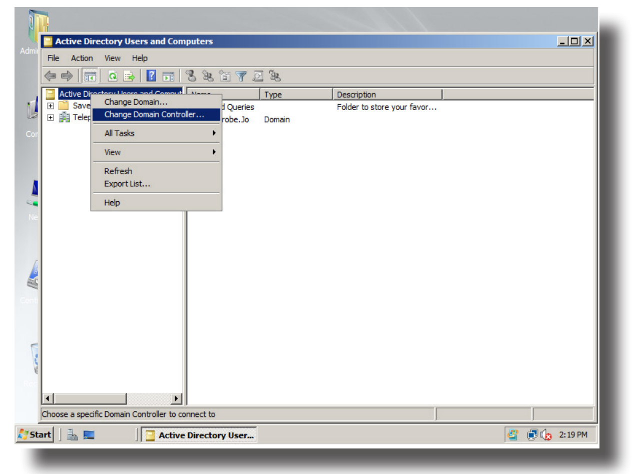
ملاحظة:

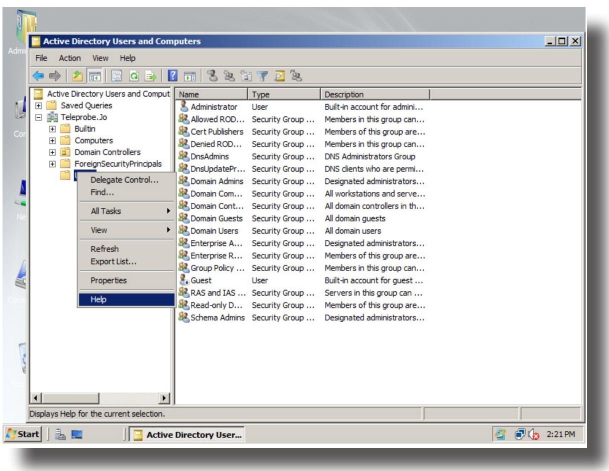
إنها مجموعة من القوائم (Wizard) عن طريق Next

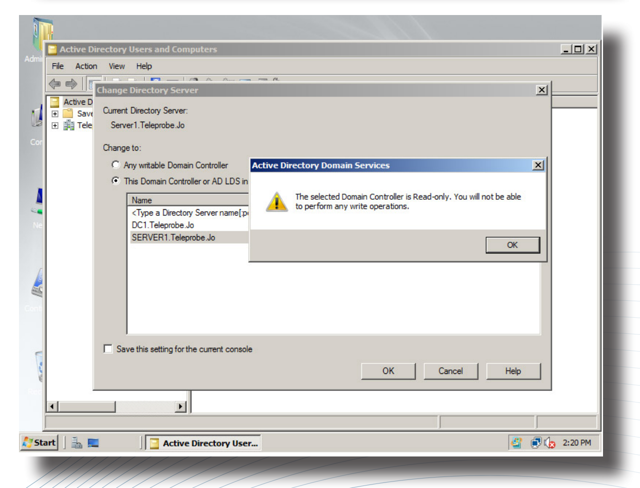
أهم هذه الخطوات التي سوف تظهر لنا و هي الصورة التالية لا تنسى أن تضع إشارة الـ (□) على الخيار Read Only Domain Controller ، و بعد ذلك نتابع تكرار الشاشات إلى كلمة Finish و عمل Reboot After Complete

بعد عملية الريستارت تكون قد أتممت خطوات التحويل إلى RODC , تبقى خطوة واحدة و هي : تغير الـ DC إلى خيار الـ RODCو ذلك عن طريق Active Directory Users and Computers









أتمنى أن أكون قد وفقت في شرح هذه الطريقة



ثالث خطوات إحتراف عملية الـ Bac up



في تدويناتي الثالثة لعالم احتراف الـBackup سوف أتناول فكرة لم يتم التطرق إليها من قبل, وتدور حول Backup rotation scheme التي وجدتُ صعوبة في تعريبها. لكن بشكل عام هي الطرق التي تحفظ نسخك الاحتياطية من الضياع من خلال عمل جدول معين لكيفية توزيع النسخ الاحتياطية على وسائط التخزين المتوفرة, لنوضح بشكل أكبر...

عندما تبدأ بعمل Backup عادة ما تعتمد على هارد أو أثنان أوثلاثة فيحفظ المعلومات بهدف عمل تأمين كبير لبياناتك من الضياع بسبب تلف أحد هذه الوسائط (ليس شرط أن تكون هاردات فقط) لذلك أوجدَ المهتمين بهذا العالم طرق قياسية يمكن الاعتماد عليها فيقوم بعمل جدول ثابت لأخذ النسخ الاحتياطية إعتماداً عليه, وهذه الطرق كثيرة وسوف نتعرف على أشهرها.

Grandfather-father-son

ابن – والد – جد , أحد أشهر الطرق المعروفة في هذا المضمار وتعتمد عليها الكثير من الشركات, آليتها تقوم على الشكل الآتي:

الابن : يقصد به النسخ الأحتياطي اليومي ويتم تخصيص أربع وسائط حفظ لهن سُجّل على كل واحدةٍ منها أحد أيام الأسبوع (الأحد, الأثنين, الثلاثاء, الأربعاء) فلو فرضنا أن الأسبوع يبدأ يوم الأحد وينتهي الجمعة, سوف نقوم بعمل نسخ احتياطي إعتماداً على أحد الطرق التى وضّحناها في المقال السابق. Incremental\Deferential ابتداءً من يوم الأحد وصولاً إلى يوم الأربعاء. وتتكررالعملية كل اسبوع بحيث نستخدم أقراص الحفظ نفسها وكل قرص له يوم محدد .

الوالد: يقصد به النسخ الأحتياطي الإسبوعي ويتم تخصيص خمس وسائط تخزين أيضا, نسجّل على كل قرص منها (الأسبوع الأول, الأسبوع الثاني, الأسبوع الثالث) ويكون اليوم الأخير من الأسبوع أي يوم الخميس هو اليوم المخصص للحفظ ونستخدم عادة طريقة الـ Full Backup.

الجد: يقصد به النسخ الاحتياطي الشهري ويتم تخصيص ثلاث وسائط تخزين نسجّل على كل قرص منها (الشهر الأول, الشهر الثاني, الشهر الثالث) بحيث يخصص لكل أربع أشهر أحد وسائط التخزين, وعلى نفس طريقة الحفظ الأسبوعي نقوم بعملية الحفظ الشهري أي Full Backup والمجموع سوف يكون اثنا عشر, أقراص حفظ ملفات الـ Backup.

Round Robin

أحد أقدم وأبسط الطرق المستخدمة, وهي تعتمد على خمس وسائط تخزين تتحرك وتتغيير بشكل أوتوماتيكي ودوري وفقاً للجدول التالي:

وسيلة التخزين	ايام الأسبوع						
	السبت	الأحد	الاثنين	الثلاثاء	الاربعاء	الخميس	الجمعة
A						X	
B					X		
C				X			
D			X				
E		X					

خمس وسائط تخزين تتحرك بشكل دوري خلال أيام العمل وعادةً تكون طرق النسخ Incremental\Deferential لأول أربعة أيام والخميس يكون Full.





Tower of Hanoi اسم لأحد الألعاب الصينية القديمة التي تعتمد على الذكاء وتقوم على مبدأ وجود خمسة أصناف من الأحجار كل حجر منها يتحرك بعدد خطوات معينة وفق عملية حسابية معينة, والتي اعتمدُ عليها لتشكيل أحد أكثر الطرق ذكاءً لعمل جدول لتوزيع وسائط التخزين, وهي تعتمد على وجود ثلاث أو أربع أو خمس وسائط وفقاً للجداول الثلاث القادمة,

ولاحظ معي أن وسيط التخزين الأول A يتحرك بشكل ثنائي أي كل يومان, وبمعنى آخر 1, 3, 5, 7 , أما وسيط التخزين B فهو يتحرك أربع خطوات, والقاعدة العامة لطريقة التوزيع مبنية على قاعدة علمية رياضية. لم أشأ الدخول فيها كثيراً وفضلت نقل الجدول الذي يوضح توزيعات وسائل التخزين في أيام .

Three-Tape Hanoi Schedule

	Day of the Cycle							
	01	02	03	04	05	06	07	08
Set	A		A		A		A	
		B				B		
				C				C

Four-Tape Hanoi Schedule

	Day of the Cycle															
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Set	A		A		A		A		A		A		A		A	
		B				B				B				B		
				C								C				
								D								D

Five-Tape Hanoi Schedule

	Day of the Cycle																															
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Set	A		A		A		A		A		A		A		A		A		A		A		A		A		A		A		A	
		B				B				B				B				B				B				B				B		
				C								C								C								C				
								D																D								
																E																E

إلى هنا نكون قد أنهينا الجزء الثالث من السلسلة والتي قدمت فيها أشهر وأبسط وأذكى العمليات المستخدمة, في عمل جدول لتوزيع الوسائط التي يمكن استخدامها في عملية النسخ الأحتياطي, ومقالي القادم إن شاء الله سوف يكون حول وسائط التخزين نفسها.

تقنية الـ ZigBee





أحدثت تقنية Wi-Fi ثورة في مجال شبكات الحاسب الآلي ، حيث سهلت لنا الإتصال بالشبكات الداخلية حينما نكون بالخارج . كما سهلت لنا هذه التقنية التوصيلات بين الاجهزة . فقد قللت عدد الكابلات بشكل كبير جداً . مما أدى هذا إلى إهتمام الشركات بهذه التقنية وكذلك أدت هذه التقنية إلى جذب المستخدمين المنزليين لإستخدامها . فقد بدأت الشركات بالتطوير التقنيات اللاسلكية ، حيث تعددت التقنيات اللاسلكية بمختلف تردداتها مثل :

- تقنية Bluetooth .
- تقنية GSM .
- تقنية CDMA .

ولكن في تلك الأثناء كانت هنالك الكثير من الشركات والمؤسسات تعاني من مشكلة إستهلاك الطاقة وكلفة بناء المشاريع بهذه التقنيات . كما كانت هنالك شركات ومؤسسات تعاني من مشكلة كبيرة جداً . وهي أن عطل جهاز واحد يؤدي إلا توقف عمل الأجهزة الاخرى .

ومن ذلك المنطلق بدأ المهندسين يفكرون بتقنية جديدة بحيث تكون مستهلكة للطاقة بنسبة طفيفة وتكلفة تصنيعها رخيصة. فقد شاهد المهندسين حركة النحل عندما تجتمع مع بعضها البعض ، تستطيع أن تؤدي مهمات معقدة وصعبة بمشاركة كل نحلة بطاقتها البسيطة . كما لاحظوا أيضاً أن النحل يستخدم لغة ورقصة خاصة بها لتتعارف فيما بينها .

ومن هنا أبتكر المهندسين التقنية الجديدة التي أطلقوا عليه أسم (ZigBee) ، أي دوي النحل أو اللغة التي المستخدمة من قبل النحل لتخاطب فيما بينها للقيام بمهمة معينة .

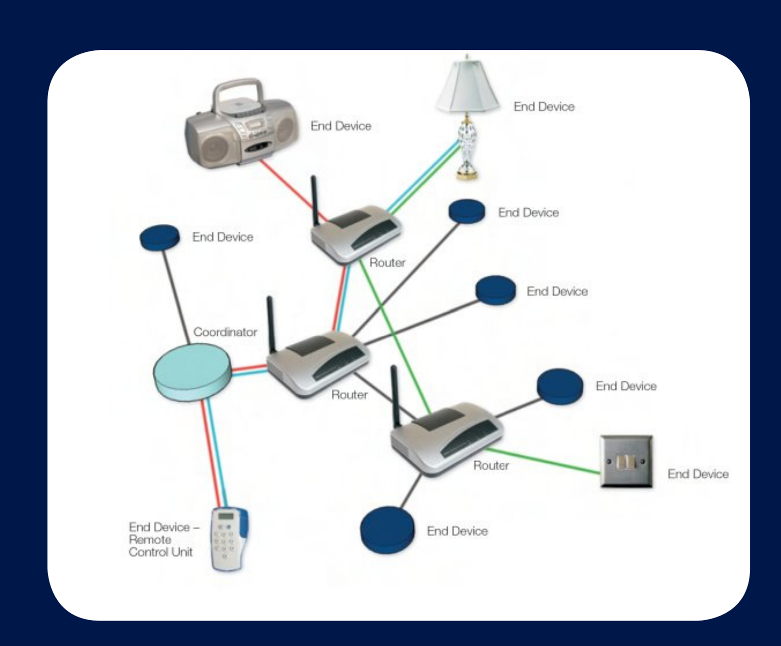
ما هي تقنية الـ ZigBee ؟



هي تقنية ربط شبكي صممت خصيصا للإستخدامات التي تحتاج إلى ربط شبكي يعمل لفترات طويلة دون الحاجة للتزويد بطاقة كهربائية بين فترات قصيرة. حيث زودت هذه التقنية ببطاريات فترة حياتها تصل الى 360 يوما من العمل بشكلٍ متواصل دون الحاجة لشحنها سواء مرة واحدة . كذلكً صممت خصيصاً للإستخدامات التي تحتاج إلى توفر الخدمة بدرجة عالية بحيث يكون هنالك بديل مباشر في حال تعطل أحد الأجهزة.

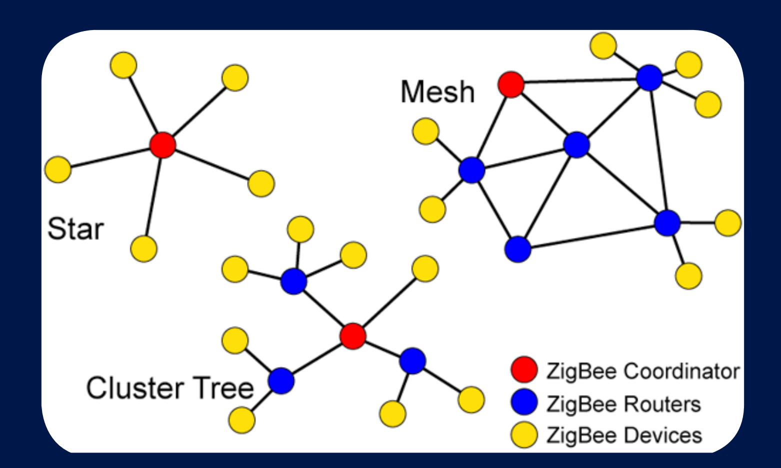
ولم تركز الشركات المطورة تركز في تطوير هذه التقنية بحيث تكون استخدامها للمؤسسات والمشاريع بل طورتها ليمكن إستخدام هذه التقنية في أيضاً في المنازل بحيث توفر ربط شبكي لأجهز التبريد والتسخين وغيرها من أجهزة منزلية ترفيهة لتكون لها وحدة تحكم مركزية . والجدير بالذكر أن هذه التقنية توفر المرونة لتوسعتها بسهولة وتتميز أيضاً بأنها توفر حماياتها قوية .

وتندرج هذه التقنية ضمن المعيار (IEEE 802.15.4) وتستخدم ترددات مختلفة حسب تصنيفها في الدول مثل التردد MHz 902 و MHz 868 .
وتوضح الصورة التالية أستخدام هذه التقنية في المنازل لربط الاجهزة المنزلية :



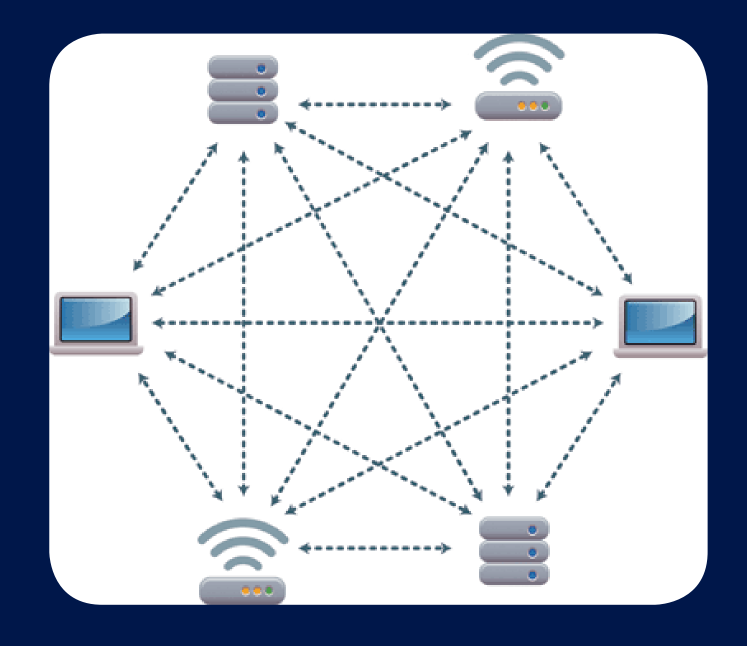
بنية تقنية تقنية الـ ZigBee وعناصرها :

تتكون هذه التقنية من عدة عناصر رئيسية حيث أن هذه العناصر تكون موصولة فيما بينها بعدة أنواع من التوبولوجيا مثل (Star, Cluster-Tree, Mesh) كما في الصورة التالية :



ولكل عنصر من هذه العناصر المرتبطة مع بعضها البعض وظيفة معينة . حيث أن الـ Coordinator مسؤول عن بدء العمل في الشبكة والتحكم بها . كما أنه يخزن المعلومات عن الشبكة والتي تتضمن معلومات عن الحماية والمراكز الموثقة للبث. أما الـ Routers فهو المسؤول عن عملية توسيع الشبكة بطريقة ديناميكية وعن توفير نسخة من اعدادت الراوترات وايضا توفر تقنية Fault Tolerance أي عدم توقف الأجهزة الأخرى في حال توقف أحد الأجهزة . أما عن Devices فما هي إلى الأجهزة التي تستقبل وترسل فقط .

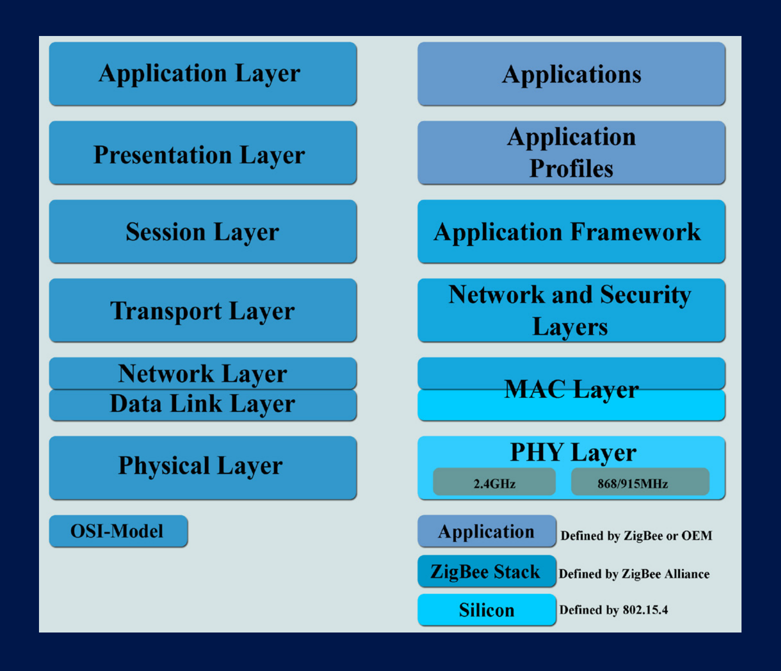
والأكثر شيوعا في ربط عناصر تقنية الـ ZigBee يكون بتبولوجيا الـ Mesh كما هو ظاهر في الصورة التالية :



وتتميز هذه التبولوجيا بأنه أكثر ضماناً لوصول البيانات كما أنها صعبة الإنهيار . بالإضافة إإلى قردتها على إتاحة لنا القضاء على مشكلة أجزاء الشبكة المتوقفة عن نقل البينات او الضعيفة في نقل البيانات بمعالجتها بكل سهولة وذلك بإضافة راوتر جديد موصول بهذه الأجزاء لتكوين جزء جديد يساعد على زيادة أداء الشبكة . ومن المهم ذكره أن هذه التبولوجيا تتميز عن بقياتها ، حيث أن عند توقف أحد الاجهزة عن العمل او عطل في التوصيل ، تستطيع نقل البيانات بإستخدام الأجهزة الأخرى المرتبطة بالشبكة.

نموذج تقنية الـ ZigBee ومقارنته مع نموذج الـ OSI :

أن تقنية الـ ZigBee تمتلك أيضاً نموذجاً خاصِ بها يصف كل طبقة ووظيفتها كما هو الحال في نموذَج الـ OSI :



الحماية في تقنية الـ ZigBee :

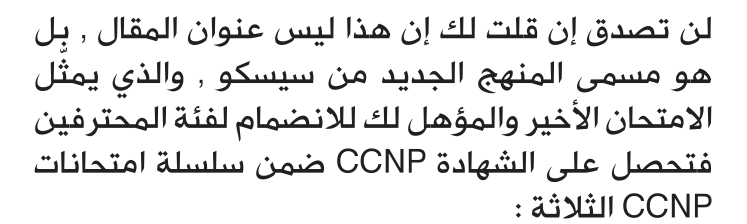


تمتلك هذه التقنية 3 مفاتيح للحماية لكل واحد منها دوره الخاص . وهذه الأنواع مبنية على 128-bit AES . فهنالك نوع يسمى Network Key يقوم بعمل حماية على طبقة الشبكة . وتستخدم جميع الأجهزة المرتبطة هذا المفتاح للإتصال فيما بينها لتقوم بتشفير بياناتها. أما Master Key فهو يولد مفاتيح أختيارية لا تستخدم لتشفير الفريمات وإنما تستخدم لتوليد مفتاح سري يتم التشارك به بين جهازين . والنوع الثالث هو Link Key وله علاقة بالمفتاح السابق ويستخدم لعمل Unicast Message .

البروتوكولات التي تعمل في تقنية الـ ZigBee :

كما نعلم ان هنالك الكثير من البروتوكولات الشبكية . وأن البروتوكولات هل لغة التخاطب بين الخدمات الشبكية . ولكل برتوكول وظيفته الخاصة . حيث تمتلك تقنية الـ ZigBee الكثير من البروتوكولات التي تعمل علة إنجاز خدمات هذه التقنية . يوضح النموذج التالي هذه البروتوكولات :





صيانة وحل مشاكل شبكات سيسكو

Troubleshooting and Maintaining Cisco IP Networks

لن تصدق إن قلت لك إن هذا ليس عنوان المقال , بل هو مسمى المنهج الجديد من سيسكو , والذي يمثّل الامتحان الأخير والمؤهل لك للانضمام لفئة المحترفين فتحصل على الشهادة CCNP ضمن سلسلة امتحانات CCNP الثلاثة :

1 - الروتنج Routing
2 - السويتشنج Switching
3 - التي شوت TSHOOT

فاليوم أحببت أن نتناقش حول هذا المنهج ولاب (الامتحان) الخاص به TShooT Exam Lab ، وهذا بسبب كثرة التساؤلات حول هذا المنهج , والذي ليس فيه من الإضافات على منهجي الروتنج والسويتشنج كما يقولون إلا القليل , وهذا ما يجعل عندنا علامات استفهام كبيرة ؟؟؟ إجابتها وبكل بساطة -> نعم , لا توجد إضافات كثيرة في هذا المنهج , لكن فيه الكثير من حيث تنمية الوعي في تنفيذ الصيانة الدورية الوقائية , وحل المشاكل (لاحظ أنهما نقطتين صيانة دورية وحل مشاكل) ، كما أن امتحانه يعد كاسر لحاجز الامتحانات التقليدية من سيسكو في الشهادات Associate و Professional والانتقال نقلة نوعية وتاريخية في شكل الامتحان ليشبه امتحانات الشهادة CCIE مع الفارق الكبير طبعاً ...

أولاً وقبل أن ندخل في التفاصيل , أريدك أن تقرأ معي ماذا كتبت سيسكو في وصفها لهذا المنهج وامتحانه : إن اجتيازك لهذا الامتحان يعني أنه لديك من المعلومات الهامة والمهارات اللازمة مما يكفي لوضع وتنفيذ خطة الصيانة الدورية على مشاريع الشبكات المعقدة من سويتشات وروترات و وحل مشاكل التشغيل الروتينية منها والطارئة بطريقة علمية ومنهجية ITIL ... وهذا أهم ما في الأمر , ولا يلتفت إليه الكثير من المهندسين , بل ويظن البعض أن فائدة هذا الكورس هو فقط التدريب على حل المشاكل كما هو مشهور ؟!؟!؟! هذا بخصوص المنهج , وفي عجالة أترك لكم تفحص الكتاب والذي يستحق القراءة فهو حقيقة يرتب لك أفكارك ...

أيضاً من المناسب هنا التطرق لنقطة النقلات النوعية لسيسكو في مناهجها وشهاداتها وتسلسلها وطريقة



الحصول على تلك الشهادات ... فأنا كنت ولازلت وسأظل (ابتسامة) من المعارضين بشدة للمسار الرأسي في الحصول على شهادات سيسكو , فلا يصح إلا الصحيح , فالمسار الأفقي هو الأفضل وبلا منازع ، فإن أتى شخص ليحصل على شهادة CCNA -> CCNP -> CCIE , لاشك أنه سيكون عنده من الثغرات الشيء الكثير , ستقول لي : مع أنه حاصل على CCIE, أقول لك : نعم وإن كان حاصل على CCIE، فالشخص الحاصل على CCNP ليس عنده التصور الكامل لشيئين : الأول- ما يحدث في مزود الخدمة SP , أما الثاني- التصميم الكامل والمتصل بالشبكة From-end-to-end , ولهذا هو في حاجة إلى أن يكمل هذا الفهم والتصور بمسارين آخرين هما -> CCDA و CCDP , CCIP أولاً قبل الدخول للمستوى الثالث من شهادات سيسكو CCIE ، وصدقني عندها سيكون الحصول على CCIE سواء في الروتنج والسويتشنج أو مزود الخدمة أو التصميم سيكون من السهولة بمكان صحيح في النهاية أننا وصلنا للنتيجة نفسها , وهي ثلاثة CCIE لكن إليكم الدليل على كلامي هذا ...

هو أن سيسكو كان هذا فهمها , لكنها وجدت أن تأكيدها على أن يكون المهندس مثقفاً بجانب كونه متخصصاً وذلك بأن يحتوي المنهج على أشياء أخرى وبشكل موجز , أدى إلى ضياع الهدف الأساسي وهو مهندس

متخصص متقن , فقررت التركيز على التخصص والثقافة تترك للشخص ليعتمد على نفسه واجتهاده ، لذا بدأت سيسكو في الفترات الأخيرة تعدل من مسارها وهو المهندس المتخصص أولاً ثم المثقف يأتي بعد ذلك لتؤكد على أن الأهم أن تكون متخصصاً ، وفي النهاية الخلاف في الرأي لا يفسد للود قضية ...

نذهب الأن لامتحان TSHOOT وهنا تأتي المعضلة ؟ فكثير من المهندسين دخل هذا الامتحان ورسب , مع أني استطيع القول أنّ مستواه جيد كما أنّه قد اجتاز الامتحانين لـ الروتنج والسويتسنج ، والبعض يخاف من الدخول أصلاً . ولا أخفيكم حتى أني بعد محاولات كثيرة استطعت أن أنشئ لاب مثل اللاب الخاص بالامتحان (كما قلت لكم الامتحان كله عملي) , وبمساعدة بعض الأصدقاء , مع أني كنت أظن أن اللاب بسيط لكن وجدت فيه بعض العقبات ولا أخفيكم ذلك ...

ملحوظة : سأرفع لكم اللاب وإن شاء اللّه تستفيدون منه ... لكن بعد أن تقرأ بعناية النصائح التالية (هناك كلام وملاحظات بين السطور القادمة قد تجدها تافهة لكنها كانت السبب في رسوب البعض فأنصحك ثانية اقرأ بعناية) ...

فهيّا بنا نكسر تلك الرهبة عند البعض بهذا الموضوع , فكونوا معنا ...

الامتحان يحتوي على:

1) سؤال سحب وإفلات <-Drag and Drop
وتحتوي على ثلاثة أسئلة في قاعدة بيانات الأسئلة تقريباً , ينوع بينها ...ذكر ذلك في بعض المواقع , سأذكر الرابط في نهاية الموضوع...

2) سؤالين اختياري من متعدد اختيار واحد أو أكثر- > و تحتوي على ستة أو سبعة أسئلة في قاعدة بيانات الأسئلة تقريباً , أيضاً ينوع بينهم ... ذكر ذلك في بعض المواقع , سأذكر الرابط في نهاية الموضوع...

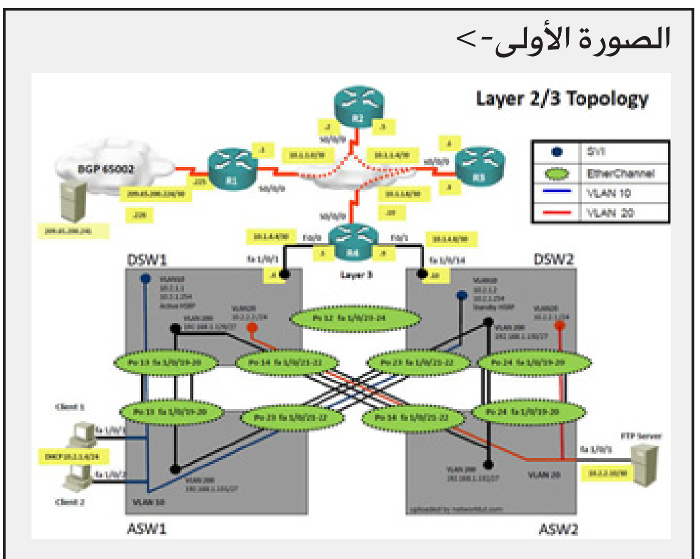
3) باقي الأسئلة12 Troubleshooting Tickets
-> نعم 12 مشكلة أو تذكرة , وكأنّه لديك شركة حلول وأنت المهندس المسؤول عنها , وأتت إليك شركة وعندها مشكلة في الشبكة الخاصة بها وأنت تقوم بحل تلك المشكلة ، يعني المريض قطع تذكرة ودخل عليك , يا دكتور الشبكات (ابتسامة) اكتب الدواء لو سمحت...

الـ 12 تذكرة أو الـ 12 مشكلة تحاول حلهم مع نفس اللاب ، نعم هي نفس الشبكة في كل المشاكل , نفس التصميم , ونفس الإعدادات , فقط مكان المشكلة مختلف ، في كل مرة يقوم بتغيير أو التلاعب في الإعدادات ,فمثلاً : يقوم بحذف الإعدادات في مكان معين ,أو يغيرها , أو يقوم بإضافة شيء خطأ , المهم يجعل في الشبكة مشكلة ما , وأنت تكتشف يا دكتور الشبكات ... شخّص وعالج !

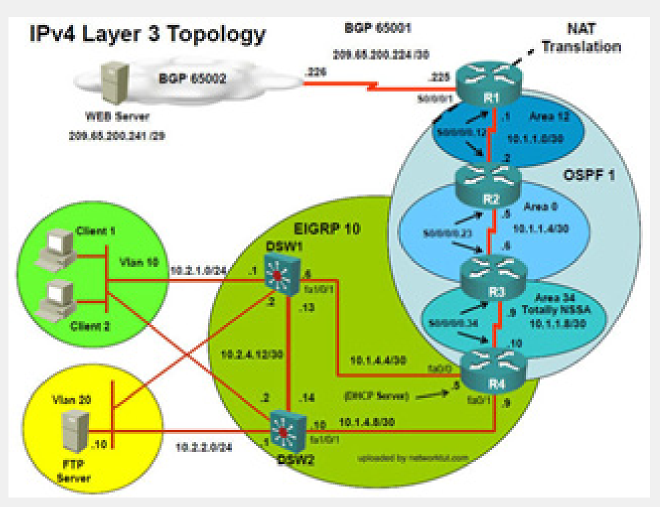
لذلك كان أحد أهم عوامل النجاح هو تصميم اللاب وإتقانه كما ذكر ذلك أخونا م.أيمن النعيمي في حديث له عن ذلك الامتحان , فقد كان محقاً ...

وهذه التذاكر هي لُب الامتحان , وعليها يتوقف نجاحك . لكن قبل أن أتعرض بشيء من التفصيل حول التذاكر , دعني أعرض تصميم الشبكة من خلال بعض الصور وإن شاء اللّه تستفيدون منها ...

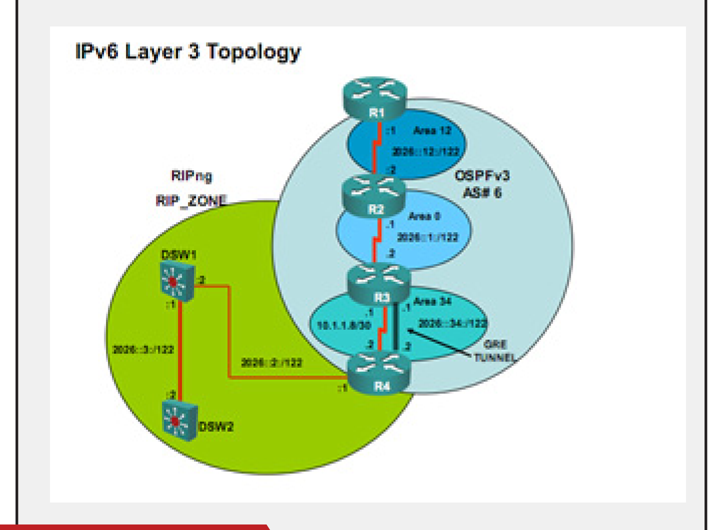
الصورة الأولى->



الصورة الثانية->



الصورة الثالثة->



أيضاً بعض المواقع استطاعت أن تخترق الإمتحان, وتجلب لك التذاكر الـ 12 ولكن ...
وأقولها بملء فمي حتى لو كنت على علم مسبق بالأسئلة التي ستطرح في الإمتحان , فلن تستطيع أن تنجح والسبب هو : أن ترتيب التذاكر يتغير , بمعنى آخر يجب أن تكون متيقظ بشكل جيد , أي مذاكر بعناية لكل تكنولجي , وتعرف كيف تعدها وتشغلها , وبالتالي تكتشف مكان الخطأ بكل سهولة , والأهم من ذلك أنك أنشئت اللاب الخاص بالامتحان وفهمته بشكل جيد ...
لذا فإن أفضل طريقة للحل هي try pinging to all the devices نعم تحاول أن تعمل بينج ping من جهاز العميل Client إلى أن تصل إلى الخلل , و أقصد هنا الجهاز الذي لا يجيب , ومن هنا تعرف مكان المشكلة until you don't receive the replies, وعندها تبدأ في العمل على هذا الجهاز لتكتشف نوعية الخطأ ...
وهذا الرجل حقيقة أبدع في وضع الطريقة الإستراتيجية التي ستحل بها الامتحان , وإليكم روابط الفيديو على اليوتيوب (ملاحظة هامة: أجمل ما في تلك الطريقة التي وضعها , هو أنه لاحظ أنّه يمكنك أن تغلق التذكرة إن استعصى عليك حلّها , لتبدأ في تذكرة أخرى ومن ثم تعود للتذكرة التي استعصى عليك حلها , ومن هنا بنى هذا الرجل إستراتيجيته في الحل , حيث أنّه وبعد أن يكتشف مكان الخطأ يغلق ويذهب لتذكرة أخرى وعندها سيجد حتماً حل مشكلته التي اكتشفها حيث أن سيسكو سترجع تلك الإعدادات لحالها لتلعب في مكان آخر فتحدث فيه مشكلة أخرى في تذكرة جديدة !!! يا للعبقرية فعندها تتأكد من كون حلك صحيح) ...
الملف الأول
http://www.youtube.com/watch?v=3Bo4Pw82G2M
الملف الثاني
http://www.youtube.com/watch?v=ZIRxfxeTSLI&feature
الملف الثالث
http://www.youtube.com/watch?v=BocjkJ1l71k&feature أرجو أن تشاهد الفيديوهات الثلاثة بعناية كاملة ولأكثر من مرة ...
الأمر الثاني والأهم هو عن أي شيء يسأل ؟ قد يسألني ما هي المشكلة ؟ قد عرفناها ... لكن هل يطلب مني حلها بعمل Configuration كما يظن معظمهم ذلك ؟ لا لا لا ... إذن ماذا يطلب ؟ وعن ماذا يسأل ؟ وكيف ؟
كل مشكلة يسألك عنها ثلاثة أسئلة : وكلها اختياري ...
السؤال الأول : أي جهاز هو سبب المشكلة , وبصيغة أخرى أين تقع المشكلة في أي جهاز Device , وطبعاً هذه سهلة ستعرفها من خلال عمل بينج Ping على كل جهاز في الشبكة من خلال جهاز العميل , فالجهاز الذي لا يجيب يكون مكان المشكلة...
السؤال الثاني : الخطأ في أي تقنية ؟ في الإعدادات الخاصة ؟ بماذا Technology , وهذا ستعرفه من خلال نتيجة أوامر الـ show وفهمك لكل تقنية درستها في كورس CCNP ...
السؤال الثالث : كيف تستطيع حل هذه المشكلة أو إصلاحها في شكل سؤال واختيارات , وهذا ستعرفه طبعاً من خلال دراستك وفهمك لكل تقنية وإعدادها وتحليلك الجيد لنتيجة الأوامر show... ويمكنك التأكد بإغلاق التذكرة للذهاب لتذكرة أخرى ورؤية الإعدادات الأصلية قبل أن يلعب فيها لتكون متيقن من حلك ...
فالأمر الغريب والذي لا يمكن توقعه في ذلك الامتحان , أنّ أوامر الـ showموجودة بكثرة !
حتى الـ debug لا يعمل بل أنتِ لا تستطيع أن تدخل إلى Configuration mode أصلاً .
أما هذا الجدول

Device	Error Description
ASW1	-Access port not in VLAN 10 -Port Channel not allowing VLAN 10 -Port Security
DSW1	-HSRP track 10 -VLAN filter
R1	-Wrong IP of BGP neighbor -NAT – Access list mis-configured -Redistribute access-list -OSPF Authentication
R2	-IPv6: enable OSPF
R3	-EIGRP – wrong AS -Redistribute

وهذا جدول أتى في بعض المواقع ليحدد لك المشاكل الإثنا عشر , وأماكن وجودها , وفي بعض المواقع الأخرى يسئلونك عن كيفية حلّها لكن المشكلة الأكبر كانت فيً ... نعم إنّ معرفة ذلك لا ينفع , لإن ترتيب التذاكر يختلف ! وبالتالي ستكون عملية التنبؤ أو حفظ الأسئلة وإجاباتها كما يفعل البعض صعبة !



أما عن أسئلة السحب والإفلات...

فهذا رابط تكلم عنها

http://www.networktut.com/tshoot-drag-and-drop-questions

وأما عن أسئلة الإختياري...

فهذا رابط تكلم عنها

http://www.networktut.com/tshoot-multiple-choice-questions

وأريد أن أنبهك إلى أن تقرأ التعليقات من القراء في ذلك الموقع فهي مفيدة جداً ...
أما الآن أتينا إلى حسن الختام وهو اللاب , وأنا راجعته مع بعض المواقع مثل الموقع السابق , والحمد لله وجدته نفسه وإليكم الرابط من الموقع المذكور

رابط التحميل (اللاب مصمم على برنامج الـ Packet Tracer)

http://www.networktut.com/download/TSHOOT_LAB.pkt

ولا أنسى ولا يفوتوني هنا أن أجعلك تدخل و تجرب الامتحان بنفسك وترى كيفية التذاكر tickets , لتتدرب على طريقة الإمتحان ... فهذا نموذج للإمتحان (تجريبي) يعني من سيسكو ...

http://www.cisco.com/web/learning/le3/le2/le37/le10/tshoot_demo.html

ولا تنسى أن التذكرة إن أغلقتها «راحت عليك يا حلو» (ابتسامة)

عدد أسئلة الامتحان إجمالاً 15 سؤال...
وزمن الامتحان 155 دقيقة للناطقين باللغة الإنجليزية , أما غير الناطقين باللغة الإنجليزية العرب مثلاً يضاف لهم 30 دقيقة ليصبح

Total Session Length with adjustment (in minutes): 185

في النهاية أرجو أن أكون قد استطعت أن أفيد الجميع , وهذا من خلال خبرتي المتواضعة...
باللّه عليكم لا تنسوني من صالح دعائكم فأنا بحاجة إلى الدعاء وجزاكم اللّه خيراً ورمضان كريم ...



Magazine

NetworkSet

First Arabic Magazine For Networks